MODEL-BASED SYSTEMS ENGINEERING FOR DESIGN, MANAGEMENT, AND GOVERNANCE OF PROTECTIVE SYSTEMS

A Dissertation

by

DIANA GALLART HAMILTON

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Martin A. Wortman
Committee Members,	Antonio Arreola-Risa
	M. Sam Mannan
	Paul Nelson
Head of Department,	Valerie Taylor

May 2017

Major Subject: Interdisciplinary Engineering

ABSTRACT

The failure of protective systems can be catastrophic, and has its origin in management. Yet, most engineering works regarding protective systems focus on their physical components. Historically, protective systems have relied on a document-based approach, which implies handling several disjointed artifacts that are expensive to maintain and have a high potential for inconsistency and obsolescence.

We present a framework that embeds management and governance in protective systems and harmonizes regulations, theories, and inconsistent industry guidelines. It pioneers the modeling of protective systems according to the tenors of model-based systems engineering (MBSE), which significantly reduces the pitfalls of its document-based counterpart. It provides a realistic approach to manage multiple aspects of change, and offers traceability, simulation, and visualization capabilities.

First, we sketched a conceptual model that encompasses the physical components, management system, policy, laws and regulation, stakeholders and lifecycle, and stresses the importance of understanding the interactions among elements and their dynamic nature. Then, we used it as a baseline to develop the structure and behavior of our computerized model in SysML.

Our MBSE framework advances the state of the art in safety-critical protective systems by integrating management and governance, and offering further capabilities inherent to the MBSE approach. It is suitable for combined design, operation, and regulation; it reduces the cost of maintenance of its artifacts; and it offers tools for simulation, impact analysis, and management of change. It supports shared governance and mitigates information asymmetry.

Potential users include both enterprises and regulators from the chemical process safety

industry and the energy sector, and any other agents invested in the design and management of protective systems.

The model of protective systems developed in this research conforms to the standards issued by the Object Management Group (OMG) and the International Council on Systems Engineering (INCOSE). We believe that it may constitute a beginning point in the development of more sophisticated standards and both prescriptive and performance-based regulation for protective systems, intended to prevent catastrophic failures. It may also help regulators to synthesize and disseminate information, as they serve as an interface and mediator between companies and the general public.

DEDICATION

To those who have made me become who I am. To those who inspired and supported me; to my former professors and my future students.

ACKNOWLEDGMENTS

I would like to thank my chair Dr. Martin A. Wortman, for all his guidance, time and patience throughout my doctoral studies; as well as my committee members: Antonio Arreola-Risa, M. Sam Mannan, and Paul Nelson, for their support and advice.

Special thanks to Dr. César O. Malavé and the Industrial and Systems Engineering Department of Texas A&M University, for making possible the acquisition of the software tools used in this research.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supervised by a dissertation committee consisting of Professor Martin A. Wortman (advisor), of the Department of Industrial and Systems Engineering; Professor Sam Mannan, of the Department of Chemical Engineering; Professor Paul Nelson, of the Nuclear Engineering Department of the Dwight Look College of Engineering; and Professor Antonio Arreola-Risa, of the Information and Operations Management Department of the Mays Business School.

All work for the dissertation was completed independently by the student.

Funding Sources

Graduate study was supported by a scholarship from the Mexican National Council of Science and Technology *Consejo Nacional de Ciencia y Tecnología (CONACyT)*, a complementary scholarship from the Mexican Ministry of Public Education *Secretaría de Educación Pública (SEP)*, and *Tecnológico de Monterrey Campus Estado de México*.

NOMENCLATURE

ACT	Activity Diagram
AIChE	American Institute of Chemical Engineers
BDD	Block Definition Diagram
BPMN	Business Process Model and Notation
CCPS	Center for Chemical Process Safety
CFR	Code of Federal Regulations
DoD	Department of Defense
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effect Analysis
HROs	High Reliability Organizations
I&E	Instrumentation and Electrical
IAEA	International Atomic Energy Agency
IBD	Internal Block Diagram
IBM	International Business Machines
ICS	Incident Command System
IDEF	Integration Definition

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council on Systems Engineering
IPLs	Independent Protection Layers
IPS	Instrumented Protective Systems
ISA	Instrumentation, Systems and Automation
ISO	International Organization for Standardization
LLC	Limited Liability Company
LOPA	Layer of Protection Analysis
LPG	Liquefied Petroleum Gas
MARTE	Modeling and Analysis of Real Time and Embedded Systems
MBSE	Model-Based Systems Engineering
MOC	Management Of Change
NASA	National Aeronautics and Space Administration
NGOs	Non-Governmental Organizations
OMG	Object Management Group
OOSEM	Object-Oriented Systems Engineering Method
OSHA	Occupational Safety and Health Administration
PAR	Parametric Diagram

PKG	Package Diagram
PRA	Probabilistic Risk Assessment
PSM	Process Safety Management of Highly Hazardous Chemicals
QRA	Quantitative Risk Assessment
REQ	Requirements Diagram
RFC	Request For Change
RMP	Risk Management Plan
SD	Sequence Diagram
SE	Systems Engineering
SoaML	Service Oriented Architecture Modeling Language
STM	State Machine Diagram
STUK	Radiation and Nuclear Safety Authority (in Finland)
SysML	Systems Modeling Language
SYSMOD	Weilkiens System Modeling
TRI	Toxic Release Inventory
UML	Unified Modeling Language
UPDM	Unified Profile for DoDAF/MOD
U.S.	United States
U.S.NRC	U.S. Nuclear Regulatory Commission
US$	United States Dollar

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

1. INTRODUCTION

1.1 Statement of purpose

The design and operation of protective systems in safety-critical enterprises is complicated by the diversity of technologies, stakeholders, and managers. Hence, developing design and operations protocols that advance the efficacy of protective systems remains a formidable engineering challenge. Catastrophic failures of protective systems have their origin in management failure: failure to manage design, operations and maintenance, and their multiple forms of change.

Historically, protective systems have relied on a document-based approach, which implies handling a large number of disjoint artifacts. Maintaining those artifacts is expensive, time consuming, and has a high potential for inconsistency and obsolescence, aggravating the problem of deficient management of change (MOC). MBSE is a relatively new concept, which emerged within the last decade in the aerospace industry. Among its benefits, it significantly reduces the limitations inherent to its document-based counterpart. It has been successfully applied in other technologies, but not yet in protective systems.

We introduce the application of modern principles of MBSE to protective systems, provide a framework for their management and governance throughout their lifecycle, and offer tools beneficial in the MOC.

1.2 Research contributions

This research work presents a framework that embeds governance in protective systems, and harmonizes regulations, theories, and inconsistent industry guidelines. It pioneers the modeling of protective systems according to the tenors of MBSE. It provides a realistic approach to manage multiple aspects of change, and offers traceability, simula-

tion, and visualization capabilities.

1.3 Roadmap to this dissertation

This dissertation is divided in five major sections. Section 1 gives an overview of the problem and its importance, summarizes some of the related existing work and gaps, and explains the role of protection in mitigating moral hazard. Section 2 provides a framework for the MBSE approach followed in this research and the current characterization and management of protective systems, as well as a literature review on the topics covered in the introduction. Section 3 presents a conceptual model of protective systems, describing its main components, and stresses the need to understand the interactions among the elements and their dynamic nature. Section 4 describes the model product of this research and its capabilities, and Section 5 concludes with a description of future work and further challenges.

1.4 Overview of the problem and its importance

1.4.1 Historical catastrophic events where protective systems failed and third parties were affected

Every year safety-critical incidents happen in various types of industries throughout the world. While many events are considered "near misses" as they result in no damages, others have significant costs beyond the business interruption losses[1], including property damages, environmental damages, and injuries, or even fatalities, among both plant workers and civilians who may or may not be aware of the risks imposed on them. Therefore, they have economic and moral implications.

[1] In the energy sector, business interruption claims after losses are typically two or three times the size of the property-loss value, but can be much higher [57].

In the last few decades, various incidents with major consequences to the enterprise and its near -and not so near- neighbors have taken place: nuclear disasters, as those in Three-Mile Island (1979)[2], Chernobyl (1986)[3], Fukushima (2011)[4]; toxic vapor releases, as those in Seveso, Italy (1976)[5], Bhopal, India (1984)[6]; explosions in the petrochemical industry, as those in San Juan Ixhuatepec, Mexico (1984)[7], are examples of that.

Each of the 100 largest property-damage losses that have occurred in the hydrocarbon industry from 1974 to 2015 had a value, in 2015 U.S. dollars[8], of more than US$130 million, and they have a total accumulated value of over US$33 billion [57]. Although many other incidents with significantly less property-damage share their root causes, all of the 100 largest losses were due to a simultaneous failure of various prevention and mitigation layers in the protective process-safety management system [56]. Hence, the failure of protective systems is the real cause of catastrophes.

[2]The incident at the Three Mile Island Unit 2 nuclear power plant in Middletown, Pennsylvania, led to no immediate deaths or injuries to plant workers or members of the nearby community [44], and the Nuclear Regulatory Commission estimated that approximately one additional cancer in the area would result from it [85]. However, it affected 195,000 residents living within 32 km, who were evacuated voluntarily, highlighted challenges such as evacuation of hospitals and nursing homes [34], and resulted in damages requiring an estimated $1 billion for cleanup costs alone, of which only $300 million were covered by insurance [45]. The cleanup effort took nearly 14 years to complete [85].

[3]In the Chernobyl disaster more than 30 people were killed immediately, and 135,000 people in the surrounding 20-mile radius had to be evacuated [44]. Other sources report that 115,000 residents were evacuated in 1986, 220,000 subsequently evacuated by 1992, and 270,000 lived in contaminated area. 134 workers developed acute radiation syndrome, an increased incidence of thyroid cancer in children living nearby was observed, and long-term psychosocial effects occurred [34].

[4]An analysis of the societal consequences of this incident, including the need for decontamination, return of evacuees, health concerns and societal costs can be found in [90]. Health effects are further explained in [34].

[5]Over 250 cases of chloracne were reported, over 600 people were evacuated (several days after the release), and an additional 2,000 people were given blood tests [19].

[6]With more than 2000 civilian casualties [19].

[7]The aftermath includes 500-600 deaths, 5,000-7,000 severe injuries, 10,000-60,000 people made homeless, 31 million dollars of damages, and the destruction of 1/3 of the LPG supply to Mexico City [1].

[8]Values represent the amount of the loss at the time of the loss, converted to US$, using the exchange rate at the time of the loss, and inflated to December 2015 values.

1.4.2 The real cause of protective system failure is management failure

Behind protective systems failure there is management failure: faulty designs, careless operation by personnel not properly trained or with excessive workload, infrequent inspections, lack of preventive and corrective maintenance, lack of redundancies where needed, the use of incompatible equipment, materials or protocols after a poorly planned change, improper resource allocation, and many other issues that can cause a major incident in safety-critical companies, are originated in management.

Management is either alluded to or explicitly mentioned in the definitions of *protective system*[9], *instrumented protective systems (IPS)*[10], and *protection layer*[11], with keywords such as "implemented", "design and managed", and "supported by a management system", between the list of their various physical components and their purpose of preserving safety. Hence, protective systems and protection layers are more than simply their physical components.

While the physical components can fail and are expected to wear out at some point, despite the efforts in science and engineering[12], it is in the management dimension where the efficacy of protective systems truly resides. As Trevor Kletz, the 'founding father' of inherent safety remarks, "it isn't what you expect, but it is what you inspect". Management is responsible for conducting periodic audits and inspections to the facilities, the

[9] *Protective systems* are a collection of means or devices implemented to achieve or maintain a safer state of a system when unacceptable operating conditions are detected, to reduce the risk of an identified hazardous event [13].

[10] *IPS* are protective systems composed of a separate and independent combination of sensors, logic solvers, final elements, and support systems that are designed and managed to achieve a specified integrity level. They are used to reduce the process risk related to health and safety effects, environmental impacts, loss of property, and business interruption costs [13].

[11] A *protection layer* is "a physical entity supported by a management system, which is capable of preventing a hazardous event from propagating into an undesired consequence" [13].

[12] A significant portion of the work in engineering research associated to protective systems focuses on the physical components (e.g. the development of more resistant materials, improvements in the design of mechanical and electrical components, more accurate electronic devices, etc.). The one that impacts directly the management systems behind them, can be within, but also goes beyond the domain of industrial engineering, as it is not only related to maximizing machinery uptime, optimal maintenance policies and broader areas of decision analysis and operations research.

equipment and the procedures, scheduling maintenance and repairs, determining where redundancies are needed, designing and implementing safety programs to identify, eliminate, and ideally prevent safety hazards. "A good management process includes deciding what needs to be done, doing it, documenting that it has been done, and studying these results and improving the process" [19].

From an equipment perspective, the effectiveness of independent protection layers (IPLs) is measured by their functionality, integrity, reliability, and from a human factors perspective; but the IPLs effectiveness is limited by the management system used to ensure compliance with practices and procedures [79]. Yet, the management and governance dimensions are often overlooked, or not well integrated, in the existing characterizations of protective systems, oriented towards their physical components.

1.4.3 Challenges in the management of protective systems

Recognizing that the failure of the protective systems is the real cause of catastrophes, and that system failure is ultimately management failure, managing protective systems presents many challenges. These challenges include:

1.4.3.1 Lack of historical data

The lack of historical data on protective systems failure complicates analysis. On the one hand, it is desirable not to have any kind of protective system failure ever, due to the high consequence severity of such events. Very infrequent failures implies that major losses rarely occur. On the other hand, in order to conduct diverse statistical analyses[13], many data points are needed. Without large sample sizes, the results can be invalid or

[13]In [17] the authors used detailed data analysis including chi-square tests and proportional analysis to investigate the impact of the new OSHA crane and derricks regulations on the frequency of crane malfunctions or misuses that result on fatalities and injuries. While their research relates to impact analysis, safety regulation and risk mitigation, it is applicable to incidents in construction sites, not to the failure of protective systems in safety-critical companies.

misleading, even after using corrections. Furthermore, the scarce existing data may not always be comparable. Even when data are collected using an acknowledged failure mode classification[14], "the data may lack relevant information about the associated safety system and thus be valid for a specific system only, not for generic equipment and systems in general" [76].

1.4.3.2 Successful measures versus simply good luck

Given the distinction between an absence of initiating causes and a failure of protective systems, it is very hard to tell if the lack of critical incidents is due to success in preventive and protective measures, or merely good luck. It could be the case that the protective system was down or would have failed during a time when, fortunately, no initiating causes were present so no harm was done. Frequent testing often implies interruptions to the normal operation of the protective system or the critical technology behind it, and for this reason an apparent solution to confirm the system readiness is not always easy to implement.

Also, since they are not always used, protective systems are often unnoticed, until they are needed and fail. While many people would agree that it is always better to have working protective systems and never need to use them, rather than constantly need their use, their relatively low frequency of use and its silent, unnoticed nature are perhaps some of the reasons why, as public choice analysis show, "politicians tend to underinvest in precautionary efforts since these do not lead to substantial political gains during the term of office of the particular politician", whereas providing ex post compensation generates them high political rewards [27].

[14] Such as that adopted from the International Electrotechnical Commission standard 61508, discussed in [76].

1.4.3.3 Shared governance

IPS have many owners and operators from different disciplines, within and beyond the premises of the company, thus lacking central direction. They range from the managers at all levels and industrial organizations, to governments and regulators, first responders, and civilian organizations. Each stakeholder has a particular concern and viewpoint, often related to specific parts of the system that can be affected by others, and perhaps their participation occurs at different points in time. Therefore, besides their visible physical dimension, IPS have management and governance dimensions, and present the additional challenge of shared governance.

1.4.3.4 The dynamic nature of protective systems

Furthermore, IPS are dynamic, constantly evolving. Changes in technology, policy modifications, and personnel turnover at all levels, stress the need for an appropriate MOC, given the impact they could have in other parts of the system and the system as a whole. Not only do protective systems change whenever modifications to the protective system itself are performed, they need to be adapted as the critical technologies or the procedures that they are intended to protect change. In all cases, except for the simplest replacements in kind, the respective changes need to be assessed and approved prior to their implementation, and must be properly documented and informed to the pertinent stakeholders, who might require training as a result.

1.4.3.5 Interrelated system elements

One of the key issues that makes both shared governance and MOC so challenging is that the elements of protective systems are interrelated. Their parts and functions may be compartmentalized among the different types of owners and operators due to specialization, or for security reasons. However, changes in one part can affect others, and the

effects may not always be easily noticeable to those who originate them. Protective systems are characterized by high intricacy and complexity[15], therefore, they require means and approaches to understand, assess, and keep track of changes and their possible effects in other parts of the system, and in the system as a whole.

1.4.3.6 Safety is an emergent property

This is especially important, because safety is an emergent property, which means that it arises from the interactions among the components at a lower level of the system. Simply analyzing the safety of each one of the individual components of a larger system overlooks the hazards that emerge once those components interact. Therefore, safety must always be analyzed top-down, for the integrated system and its subsystems [51].

1.4.4 Introduction to systems engineering and MBSE versus the document-based approach

Needless to say, protective systems are systems[16]. IPS are engineered systems, since they are technologically enabled, complex, dynamic, have multiple interactions with natural systems (e.g. nuclear, chemical, ecosystems) and human systems (e.g. governmental, urban, community) and deal with multiple aspects of uncertainty. Given the multiple challenges they face, they call for a systems engineering[17] approach.

Systems engineering approaches can be either document-based, or model-based (or a hybrid of both). In the traditionally used document-based approach, there are many

[15] Intricacy refers to the number of different elements in a system, and complexity refers to the number and type of relationships between elements in a system [89]. Complexity is often viewed as a characteristic of systems in which no single individual is able to fully understand the whole system and all its parts.

[16] A system is defined as "a combination of interacting elements organized to achieve one or more stated purposes" (ISO/IEC/IEEE 15288). INCOSE defines it as "an integrated set of elements, sub systems, or assemblies that accomplish a defined objective", and remarks that "these elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements" [87].

[17] There are many definitions of Systems Engineering, as it refers to a perspective, a process, and a profession. See Section 2 for some of them.

disjoint artifacts in the form of text documents, spreadsheets, diagrams, and presentations. Maintaining them as the system changes is expensive and time consuming, and they can easily become inconsistent and obsolete. However, in the model-based approach, the main artifact is a system model, which is integrated, coherent and consistent [22], and where the emphasis is placed on evolving and refining the model using model-based methods and tools [30]. Despite all its benefits, the process safety industry is not currently taking advantage of all the capabilities that MBSE has to offer.

Systems engineering is interdisciplinary in nature, a feature that is necessary in the design and management of protective systems. Among its different approaches, MBSE has several advantages, especially in terms of maintenance, simulation and impact analysis capabilities. One of its modeling languages, the systems modeling language (SysML) allows to graphically represent the structure, behavior and requirements of a system model. This could help us to provide many views of the protective system, at different levels of granularity, and integrate the protection layers, but also their lifecycle, their stakeholders with their respective viewpoints, and other features of protective systems, in order to characterize them holistically. With the appropriate software tools and interfaces, methods and languages, in principle, it is possible to use that system model to perform simulation and impact analysis, and offer perhaps better ways to manage protective systems from the inside, but also from the outside of the company. Thus, such system model may constitute a beneficial tool for regulators, civilian organizations and near neighbors to mitigate moral hazard.

1.5 Summary of the state of the art and challenges

1.5.1 Many research works in engineering focus on physical components, not in management and governance

The simplest form of safety instrumented systems follows the classic model of sensor - logic solver - final element: sensors to detect the hazard, a logic solver to decide whether an emergency shutdown is needed, and final elements to isolate the process from the hazard. Therefore, it is not surprising that many research works in engineering focus on the physical components of protective systems. Some recent examples of that include studies on the way component arrangement affects the performance of complex safety instrumented systems[18], improved dependability through the integration of intelligent sensors[19], or even how plants should choose the proper sensors for their protective systems[20]. Several other works relate to probabilistic methods to estimate the probability of failure on demand of the protection layers, or to the measurement of the rate of spurious activation or spurious trip rate[21]. However, there are fewer research works in engineering that focus on the management and governance of protective systems. Some of them are related to the optimization of proof testing policies for safety instrumented systems[22]; administrative and regulatory issues, including contractual provisions for the supply of safety instrumented systems[23]; or monitoring human and organizational factors influencing common-cause failures of safety-instrumented systems during the operational phase[24].

[18] See [41].
[19] See [60].
[20] See [58].
[21] See [43].
[22] See [80], [53], and [52].
[23] See [21].
[24] See [66].

1.5.2 LOPA has deficiencies

Protective systems are often represented by a group of protection layers intended to reduce the frequency or consequence severity of hazardous events. Similar to the Swiss Cheese Model of Accident[25] Causation, proposed by Dante Orlandella and James T. Reason of the University of Manchester, Layer of Protection Analysis (LOPA) is one of the tools used for analyzing and assessing process risk that bases its methodology on this characterization.

LOPA is a simplified form of quantitative risk analysis that uses order-of-magnitude categories for initiating event frequency, consequence severity and probability of failure of IPLs to analyze and assess the risk of one or more incident scenarios [16]. The primary purpose of LOPA is to determine if there are sufficient layers of protection against a hazardous scenario to meet an organization's risk tolerance criteria. Since no layer is perfectly effective, sufficient protection layers must be provided to render the risk of the incident tolerable [12], [24]. For a further explanation of LOPA, see section 2.2.1.

While in principle it seems appropriate to model protective systems geographically or chronologically, based on the physical layers designed to prevent, and ultimately respond to a loss of containment due to an initiating cause, this representation does not show who the owners and operators of each layer are or who is accountable for them; therefore, it does not encompass management issues. Furthermore, it requires protection layers to be independent of the initiating cause and of each other, which in many cases is hard to achieve, particularly when they are managed by the same agent, and thus subject to common-cause failures. The assumption of independence also overlooks possible interactions among non-adjacent layers.

[25]The term "accident" is often found in the literature, even in the name of particular models or frameworks. Therefore, it appears as such in portions of this dissertation that refer to them. Nevertheless, it is worth mentioning that, given its connotation as something that happens unexpectedly, unintentionally, or by chance, we would rather use the broader term "incident", which does not suppress neither the preventable nature of the event nor the accountability of those who contribute to it.

1.5.3 The guidelines from the industry are document-based

Some well know professional institutions, experts in the topic, have issued several publications related to process safety. An outstanding example of this is the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE), with a series of over 100 books intended to provide the industry with guidelines. Among them, we have: *Guidelines for Safe and Reliable Instrumented Protective Systems* [13], published in 2007; *Guidelines for enabling conditions and conditional modifiers in layer of protection analysis (LOPA)*, [16], published in 2014; *Plant guidelines for technical management of chemical process safety* [10], with a revised edition published in 1995; *Guidelines for the management of change for process safety* [14], published in 2008; *Guidelines for auditing process safety management systems* [15], published in 2011; *Guidelines for Implementing Process Safety Management Systems* [9], published in 1994; and *Guidelines for integrating process safety management, environment, safety, health, and quality* [11], published in 1996.

Although these works are remarkable, given that they are document-based, as technology evolves and policies change, they can become outdated. Furthermore, there are inconsistencies among them[26], which makes the integration of two or more of the aspects treated in different publications more difficult. Following a model-based approach would be beneficial to address both limitations.

[26]For example, in [13], the book is organized using a project lifecycle with six major phases: (1) Planning, (2) Risk Assessment, (3) Design, (4) Engineering, Installation, Commissioning and Validation, (5) Operational and Mechanical Integrity, and (6) Continuous Improvement; whereas in [14], they choose to use the following definitions for lifecycle stages: (1) Process development, (2) Detailed design, (3) Construction and startup, (4) Extended shutdowns, (5) Operating lifetime, and (6) Decommissioning.

1.5.4 The paradigms that link management to safety do not provide a system model suitable for analyses and simulation

The paradigm of High Reliability Organizations (HROs), by Todd LaPorte, Gene Rochlin, and Karlene Roberts, of the University of California, Berkeley, has emerged from the field of organization theory, linking management to safety[27]. Although it offers best practices to take into account, it does not encompass regulatory issues, and ultimately it does not provide a model suitable for simulation and impact analysis. Many efforts derived from HROs have been recently conducted to improve emergency response, which constitutes the final, outer layer of protective systems, and concentrates a significant amount of external stakeholders, but they are often disjoint with respect to the inner layers.

In short, many research works in engineering focus on physical components, but not in management and governance. The characterization of protective systems as a group of protection layers used in LOPA overlooks their owners and operators, as well as management issues that may lead to common-cause failures, or interactions among non-adjacent layers, and thus violate the independence core attribute. The guidelines issued by regulators and industrial associations that do encompass management present inconsistencies among themselves, and are in the form of text-based artifacts, which brings several pitfalls with regard to their maintenance and integration. Other paradigms emerged from academia that link management to safety do not encompass regulatory issues, do not provide a model suitable for simulation and impact analysis, and in some cases simply focus on the outer layer of protective systems.

[27] See section 2.3.2 for further details.

1.6 A regulatory perspective

1.6.1 Moral hazard

There is no question that chemical manufacturing industries, companies in the energy sector, nuclear power generation, and many other technology-based enterprises bring countless benefits to humanity. They employ people, pay taxes, and provide us with useful goods and services. In return, in many cases, their shareholders profit. However, the activities these enterprises perform also come with risks[28]. Nuclear and radiation disasters, toxic material releases, fires, and explosions, are examples of obvious hazards inherent to these companies. Despite their relatively low frequencies of occurrence, the consequence severity of these incidents can be major when they take place. Furthermore, the costs of the consequences of these undesirable events are faced by many more stakeholders, internal and external, than merely the shareholders who profit under more favorable circumstances. Therefore, all the above mentioned companies have in common a hazard that is of major importance in this dissertation: moral hazard.

According to Paul Krugman, Nobel Laureate in Economics, the term "moral hazard" has its origins in the insurance industry, and eventually came to refer to "any situation in which one person makes the decision about how much risk to take, while someone else bears the cost if things go badly" [47]. A safety-critical enterprise poses a threat to public safety, as critical incidents could cause third party liabilities or losses, property damages, fatalities, and permanent injuries among its neighbors[29], as well as business partners and

[28] We can find in [74] many thoughts on risk and the perception of risks (e.g. the splashy and dreadful versus the ordinary, voluntary versus involuntary, moral versus immoral, detectable versus undetectable, natural versus man-made) from a variety of authors, followed by a comparison with other much more hazardous activities that yet seem to have a better reputation or acceptance among many people, in order to recognize why these industries are often target of misperceptions.

[29] In the U.S. code of federal regulation (14 CFR 401.5), "a safety-critical system, subsystem, condition, event, operation, process or item is one whose proper recognition, control, performance, or tolerance is essential to system operation such that it does not jeopardize public safety. Something that is safety critical item creates a safety hazard or provides protection from a safety hazard" [83].

financers.

Besides ending up bearing the costs of safety-critical incidents, neighbors and other parties face another disadvantage related to moral hazard: information asymmetry. In most cases, safety-critical companies possess more knowledge and information about their processes, the activities they perform, the properties of the materials they handle, and ultimately, the risks associated to their operation, than the neighbors and other third parties on which risks are imposed. In other words, the latter might have made decisions while misunderstanding, misestimating, or being unaware of the risks they could face.

1.6.2 The role of regulators and their needs

Safety-critical companies impose poorly understood risks to their near neighbors and have the potential to cause fatalities, injuries, and large property and environmental damages, thus creating moral hazard. Regulators and judges play an important role in the mitigation of moral hazard, inducing preventive and protective measures through the use of civil liability and safety regulation in its various forms: compliance-based regulation[30] (a.k.a prescriptive regulation), performance-based regulation[31] (e.g. the U.S. Nuclear Regulatory Commission (U.S.NRC) advocating for the use of Probabilistic Risk Assessment (PRA) methods [86]), and process-based regulation[32] (a.k.a. integral supervision). Given

[30] "This approach typically involves the regulator providing prescriptive standards and requirements - the same for every plant - for operators to follow. In this regime, inspection and enforcement are largely a matter of verifying compliance with these rules and penalising non-compliance" [40].

[31] Performance-based regulation is "a regulatory approach that focuses on desired, measurable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based regulation leads to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives for licensees to improve safety without formal regulatory intervention by the agency" [84]. "In this approach, licensees are required to comply with safety objectives, but have some flexibility to decide how they achieve that. Safety performance indicators are used by the regulator to observe trends in safety, and inspection activities focus on these indicators" [40].

[32] "The process approach focuses on the organizational systems that the facility has developed to assure the ongoing safe operation from the perspective of the facility's internal logic (...) It demonstrates to the regulator that they have taken a very rigorous approach to the design, implementation, and ongoing evaluation of their key processes and that they are alert to opportunities to improve their systems." [40].

the importance of their activities in order to preserve public safety, mitigate moral hazard and asymmetry of information; the number of agents that interact with them, and the financial and informational constraints they face, regulators require tools, methods, and theories that suit needs specific to their mission[33].

1.7 Conclusion to the section

In summary, the failure of protective systems, which can be catastrophic, has its origin in management failure; but managing protective systems is extremely challenging. This is not only because of the scarcity of historical data to analyze, and goes beyond the uncertainty about whether the lack of critical incidents is due to their proper functioning, or just a fortunate absence of initiating causes while they would otherwise have failed. It implies a shared governance, given their many owners and operators over time. It demands effective MOC, because of the dynamic nature of technology and human resources. There are multiple interactions among their elements; and since safety is an emergent property, the safety of their individual components does not guarantee the safety of the overall system.

At the same time, regulators need to have tools and methods to mitigate moral hazard, reduce the asymmetry of information, and induce preventive and protective measures in safety-critical enterprises.

The existing related research works in engineering focus on physical components and do not integrate management and governance; those issued by industrial associations (e.g. AIChE/CCPS), regulatory bodies (e.g. OSHA, EPA)[34], and those that emerged from other fields (e.g. HROs), offer guidelines and best practices that involve management, but do not provide the benefits of a model, and follow a document-based approach. This traditionally used document-based approach is expensive, time consuming, and prone to errors that lead

[33] See Section 2.4.2 for a literature review on this topic.
[34] Discussed in Section 2.

to inconsistency obsolescence. MBSE is a relatively new approach, not yet used in protective systems, that significantly reduces the limitations of its document-based counterpart, and has other benefits beyond maintenance, including traceability and impact analysis capabilities.

Our work presents a framework that introduces governance in protective systems, and pioneers the modeling of the multiple dimensions of protective systems according to the tenors of MBSE. It harmonizes regulations, theories, and inconsistent industry guidelines; provides a realistic approach to manage multiple aspects of change; and offers traceability and visualization capabilities.

The next section consists of a literature review and a theoretical framework for our work. Then, in section 3 we explain our conceptual model of protective systems. Later, in section 4, we develop our system model based on it. In section 5, we conclude with a description of future work and further challenges.

2. LITERATURE REVIEW

In this section we provide a theoretical framework regarding the approach suggested and used in this research (MBSE), the current characterization of protective systems and process safety management. Then, we perform a literature review on some of the topics encompassed in the introduction in order to explain them further, support the statements presented there, and establish a baseline for our work.

2.1 MBSE

2.1.1 What is MBSE?

There are many definitions of Systems Engineering (SE) in the literature.

To INCOSE, SE is "an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs" [87].

According to Howard Eisner, SE is "an iterative process of top-down synthesis, development, and operation of a real-world system that satisfies, in a near optimal manner, the full range of requirements for the system" [25].

To the U.S. Department of Defense (DoD), SE is "a methodical, disciplined approach for the design, realization, technical management, operations, and retirement of a system" [64].

To the National Aeronautics and Space Administration (NASA), SE is "an interdisciplinary management process to evolve and verify an integrated, life cycle balanced set of system solutions that satisfy customer needs" [62].

To the Federal Aviation Administration (FAA), SE is "a discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all the facets and all the variables and relating the social to the technical aspect" [28]

SE can be seen as a perspective, as a process, and as a profession. It includes technical and management processes, and constitutes an effective way to manage complexity and change [87]. In SE, the functional and performance requirements for a system are determined, documented, and verified [2].

SE approaches can be either document-based, or model-based (or a hybrid of both). The document-based approach involves many disjoint artifacts, which are expensive and time consuming to maintain, and can easily become inconsistent and obsolete. In the model-based approach, the main artifact is an integrated, coherent, and consistent system model [22], and the emphasis is placed on evolving and refining the model using model-based methods and tools [30].

MBSE is "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases" [36]. According to INCOSE's vision of SE, "MBSE is expected to replace the document-centric approach that has been practiced by systems engineers in the past and influence the future practice of systems engineering by being fully integrated into the definition of systems engineering processes" [36].

2.1.2 Benefits of MBSE

The main aim of modelling is to address the three evils of engineering: complexity, lack of understanding, and poor communications [37]. The purposes for modeling a system may include: characterize an existing system, specify and design a new or modified system, evaluate the system through system design trade-offs or impact assessments, and train users on how to operate or maintain a system [30]. Some of the benefits associated with the application of effective MBSE are: automatic generation and maintenance of system documents, complexity control and management, consistent and coherent views across the whole system architecture, traceability between all the system artifacts, simpler access to information, improved communication with a common language, and definitions of all the relevant concepts and terms used, and increased understanding of the system [37]. Besides these advantages, with the MBSE approach, the diagrams and autogenerated texts are merely views of the underlying system model, not the model itself [22]. Just as the pictures of an object taken from different angles can show its different features, not necessarily all at once, the distinct diagrams in the MBSE approach can show the structure, the behavior, and the requirements of the system model, at different levels of granularity, in an integrated way, while just one diagram does not necessarily show all the characteristics of the system model, as "no single diagram can communicate all aspects of the system or architecture" [2].

MBSE has three pillars: modeling languages, modeling methods, and modeling tools. Modeling languages constitute a standardized medium to communicate the elements of the model and the relationships among them. Modeling methods are a documented set of design tasks to ensure model consistency. Modeling tools, unlike diagramming tools that merely create shapes, allow to create a model with elements, relationships, and views, in which whenever an element on a diagram is modified, all the other diagrams that display that same element are updated instantaneously. One modeling language that is commonly

used by MBSE practitioners is the Systems Modeling Language (SysML); however, there are other graphical languages, such as UML, UPDM, BPMN, MARTE, SoaML, and IDEF, and text modeling languages, like Verilog and Modelica, that can be used in systems engineering. The methods include the INCOSE Object-Oriented Systems Engineering Method (OOSEM), the Weilkiens System Modeling (SYSMOD) method, and the IBM Telelogic Harmony-SE; and there exist a reasonable number of either free or commercial-grade modeling tools in the market, such as the following products and trademarks: Agilian, Artisan Studio, Enterprise Architect, Cameo Systems Modeler, Rhapsody, UModel, Modelio, and Papyrus [22].

2.1.3 What is SysML?

SysML is a general-purpose modeling language that supports the analysis, specification, design, verification, and validation of complex systems [30]. It provides graphical representations with a semantic foundation for modeling system requirements, structure, behavior, allocations, and constraints on system properties to support engineering analysis [63]. It originated from an initiative between OMG[1] and INCOSE in 2003, to adapt the Unified Modeling Language (UML) for systems engineering applications [37].

SysML currently has nine types of diagrams that are used to represent the structure, the behavior, and the requirements of the system. Figure 2.1 shows their taxonomy.

Block definition diagrams (BDD) are used to display elements that define the types of things that can exist in an operational system and the relationships between those elements. Internal block diagrams (IBD) show the connections between the internal parts of a block and the interfaces between them. Parametric diagrams (PAR) are used to express how one or more constraints, in the form of equations and inequalities, are bound to the properties of

[1]OMG is a not-for-profit computer industry standards consortium of computer industry companies, government agencies, and academic institutions.

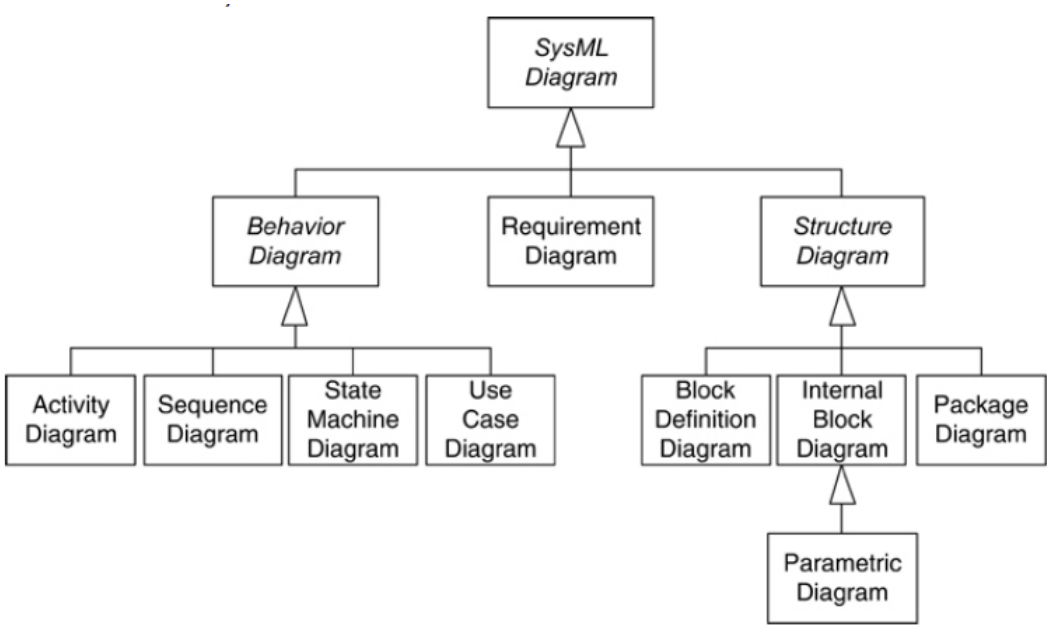

Figure 2.1: SysML diagrams taxonomy. Source: [22]

a system. They support engineering analyses, including performance, reliability, and cost, among others. Package diagrams (PKG) are used to display the way a model is organized in the form of a package containment hierarchy. They may also show the model elements that packages contain and the dependencies between packages and their contained model elements. Requirements diagrams (REQ) are used to display requirements in the form of texts, the relationships between requirements, e.g. containment, and the relationships between requirements and the other model elements that satisfy, verify, and refine them. Activity diagrams (ACT) are used to specify a behavior, with a focus on the flow of control and the transformation of inputs into outputs through a sequence of actions. Sequence diagrams (SD) are used to specify a behavior, with a focus on how the parts of a block interact with one another via operation calls and asynchronous signals. State machine diagrams (STM) are used to specify a behavior, with a focus on the set of states of a block and the possible transitions between those states in response to event occurrences. Use

case diagrams (UC) convey the actions or services that a system performs and the actors that invoke and participate in them. [22]. The SysML specification can be found in [63].

2.2 LOPA, protective systems, and management of protective systems

2.2.1 Layer of Protection Analysis (LOPA)

LOPA bases its methodology on the existence of a group of independent protection layers which conform a basic representation of protective systems. In this sense, many types of protective layers are possible [19]. Some of these layers may include: Process design, basic process control systems, critical alarms and human intervention, safety instrumented functions, physical protection (relief devices), post-release physical protection (dikes), plant emergency response, and community emergency response [19], [12]. In a broader perspective, according to the CCPS of the AIChE, the layers of protection are: Inherently safer design, control, supervisory, preventive, mitigative, barrier, limitation, and response [13].

The *inherently safer design* layer seeks to reduce or eliminate hazardous events through effective use of process technology, design methods, and/or operational techniques. The *control* layer focuses on maintaining the process within the normal operating limits. The *supervisory* layer and the *preventive* layer are designed to achieve or maintain a safe state of the process to reduce the frequency of the hazardous event. The *mitigative* layer is designed to reduce the frequency and/or consequence severity of the hazardous event. The layer of *barriers* minimizes the consequence severity due to its physical design. The *limitation* layer acts to reduce the consequence severity of the hazardous event. The *response* layer notifies personnel and/or the community to shelter-in-place or to evacuate to safe zones and musters emergency response personnel [13].

The main steps in LOPA, as described in [19], are the following:

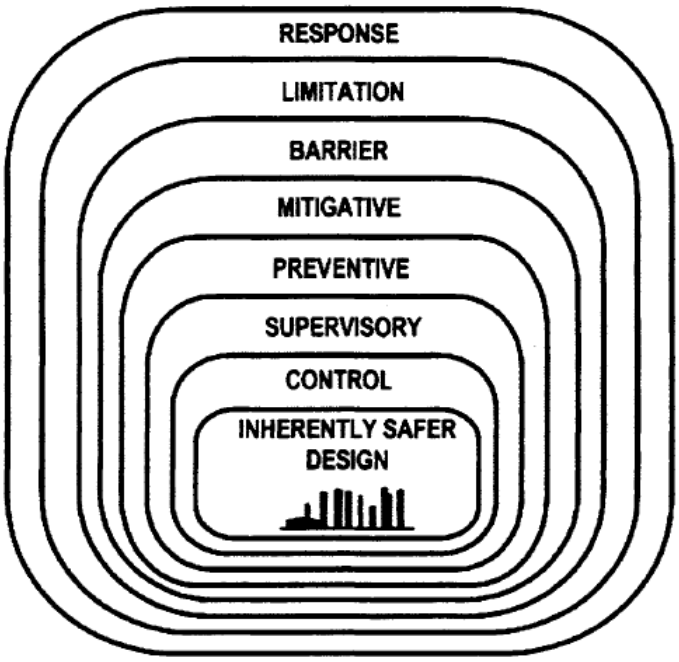

Figure 2.2: Protection layers. Source: [13]

Step 1 Identify the consequence to screen the scenarios.

Step 2 Select an incident scenario.

Step 3 Identify the initiating event of the scenario and determine the initiating event frequency (events per year).

Step 4 Identify the IPLs and estimate the probability of failure on demand of each IPL.

Step 5 Estimate the risk of the scenario by mathematically combining the consequence, initiating event, and IPL data.

Step 6 Evaluate the risk to reach a decision concerning the scenario.

The equation used for estimating the frequency of an incident scenario is:

$$f_i^C = f_i^I \times \prod_{j=1}^{i} PFD_{ij} \tag{2.1}$$

where

f_i^C is the mitigated consequence frequency for a specific consequence *C* for an initiating event *i*,

f_i^I is the frequency of the initiating event *i*, and

PFD_{ij} is the probability of failure on demand of the j^{th} IPL that protects against the specific consequence and the specific initiating event *i*.

2.2.2 CCPS guidelines

In [13], the CCPS of the AIChE establishes a framework that can be used in the design and management of IPS throughout a projects life cycle, based on International Electrotechnical Commission (IEC) and Instrumentation, Systems and Automation (ISA) standards, in order to achieve safe and reliable process operation. Besides the representation of protective systems as a group of protection layers, such as those mentioned in section 1 and illustrated in Figure 2.2, the guidelines provided in that publication include the following characteristics of protective systems:

The *core attributes* of IPS are: independence, functionality, integrity, reliability, auditability, access security, and management of change. Independence means that the performance of a protection layer is not affected by the initiating cause of a hazardous event or by the failure of other protection layers. Functionality refers to the required operation of the protection layer in response to a hazardous event. Integrity relates to the risk reduction that can reasonably be expected given the protection layer's design and management. Reliability refers to the probability that a protection layer will operate as intended under stated conditions for a specified time period. Auditability is the ability to inspect informa-

tion, documents and procedures, which demonstrate the adequacy of and adherence to the design, inspection, maintenance, testing, and operation practices used to achieve the other core attributes. Access security refers to the use of administrative controls and physical means to reduce the potential for unintentional or unauthorized changes. Management of change is the formal process used to review, document, and approve modifications to equipment, procedures, raw materials, processing conditions, etc., other than "replacement in kind", prior to implementation [13].

The *stakeholders* mentioned there are: management, process safety, process, instrumentation and electrical, operations, maintenance, and manufacturers. Management includes corporate and site organizations. It establishes policies related to safer and reliable operation, and is responsible for the oversight of the management system. Process safety includes environmental, health, and process safety management organizations, and is responsible for the process safety management. Process includes research and development, process, and process control, and its role is to design and operate the processes. Instrumentation and electrical (I&E) includes I&E, process control and reliability, and its roles encompass instrumentation and control design and implementation. Operations includes process operations and operations management; as its name suggests, it is responsible for the operation of the processes. Maintenance includes personnel from maintenance, process control, I&E, and reliability (equipment). Its role is to inspect, test, and maintain the equipment of the protective system. Manufacturers are any entity that develops, markets, and sells a product to be used in the protective system [13].

Although the guidelines in [13] imply an inside-out approach to design, operate and manage protective systems, there can also be an outside-in approach that gives more consideration to the needs and concerns of the external stakeholders that these systems are intended to protect. The behavioral theories of the firm suggest that businesses have multiple aims set by their different stakeholders, including workers, customers, local com-

munities and pressure groups, such as environmental activists, not just their shareholders and managers [32]. Besides the actively involved groups addressed in [13], in companies that perform safety-critical processes, their near neighbors are stakeholders who do not necessarily profit from the companys operations, but could be affected in the event of a protective system failure, and therefore their viewpoints should be taken into account. Sometimes that happens indirectly, through the inputs of the legislators, which may or may not overlap those of the internal policy makers in management or the process safety management organizations, and those from citizen participation groups and pressure groups. The emergency responders who would act in such events, as well as the authorities and regulators who enforce their use and inspection, are also stakeholders we should not overlook. Finally, their customers and vendors may also be affected due to business interruptions, and therefore have a stake in protective systems as well. In that sense, these other groups are considered in other publications of the CCPS. With regard to the people undertaking management activities in process safety, in [9] the CCPS classifies them into four broad groups: internal, intracompany, intermediaries, and external constituents. Internal people include the facility management group, facility safety professionals, shift supervisors, shop stewards, and employees. Intracompany people include the division president, other facility managers, and facility safety professionals. The intermediaries are the union leaders, and the regulatory authorities; and the external constituents include key customers, local officials, community activists, and neighbors. Although the emergency responders are not explicitly mentioned, except for the local officials, the last layer of protection in [13], i.e. emergency response, includes their role.

In SE, the *lifecycle* refers to the entire spectrum of activity, from the identification of needs to the system retirement and material disposal [5]. A generic system lifecycle includes the stages of observation, failing/concern/opportunity awareness, development, transition, operation, maintenance, enhancement, overhaul, decommission, and disposal.

The development process encompasses the needs analysis, requirements definition, preliminary design, detailed design, realization, integration and test, and implementation. NASA divides the project lifecycle into the following phases: (Pre-Phase A) concept studies, (A) concept and technology development, (B) preliminary design and technology completion, (C) final design and fabrication, (D) system assembly, integration and test, launch, (E) Operations and sustainment, and (F) Closeout [62]. Both lifecycle representations follow a "cradle-to-grave" approach. On the other hand, the CCPS organizes the protective management system lifecycle in seven major phases: (1) planning, (2) risk assessment, (3) design, (4) engineering, (5) installation, commissioning, and validation, (6) operational and mechanical integrity, and (7) continuous improvement [13]. While the activities of decommission and disposal of worn out or obsolete materials and abandonment of outdated practices are still implicit in the last two stages, this concept of lifecycle phases is consistent with the evolving nature of protective systems, as a "cradle-to-cradle" approach, which has been followed throughout this research.

2.2.3 OSHA PSM and EPA RMP

From the definition of protection layers[2], and our previous discussion about the importance of the management of protective systems, as well as the role of safety regulation, it should be clear that, besides the physical components of the protection layers and the stakeholders involved, management, governance, and regulation are essential.

In the U.S., the Occupational Safety and Health Administration (OSHA) of the U.S. Department of Labor, and the Environmental Protection Agency (EPA) are authorized by the Congress to create and enforce regulation to protect people and the environment[3].

[2]Protection layer: "a physical entity supported by a management system, which is capable of preventing a hazardous event from propagating into an undesired consequence" [13].

[3]The Department of Homeland Security (DHS) also participates in these activities, but it is beyond the scope of this research.

After having proposed a standard on July 17, 1990, holding a hearing, and receiving more than 175 comments and almost 4,000 pages of testimony, as well as almost 60 post-hearing comments and briefs, on February 24, 1992, OSHA published the final rule *Process Safety Management of Highly Hazardous Chemicals (PSM)*[4]. This standard emphasizes the management of hazards associated with highly hazardous chemicals and establishes a comprehensive management program that integrated technologies, procedures, and management practices. It was developed after the Bhopal incident to prevent similar events. The PSM standard has 14 major sections: employee participation, process safety information, process hazard analysis, operating procedures, training, contractors, pre-startup safety review, mechanical integrity, hot work permits, management of change, incident investigations, emergency planning and response, audits, and trade secrets [19], [82].

On June 20, 1996, the EPA published the Risk Management Plan (RMP) as a final rule, aimed at decreasing the number and magnitude of releases of toxic and flammable substances. The RMP is designed to protect off-site people and the environment, whereas PSM is designed to protect on-site people [19]. The RMP has the following elements: hazard assessment, prevention program, emergency response program, and documentation. The prevention program has 11 elements, compared to the 14 elements of the PSM standard: process safety information, hazard evaluation, standard operating procedures, training, pre-startup review, maintenance, management of change, accident[5] investigations, emergency response, safety audits, and risk assessment [19].

Besides OSHA PSM and the very similar prevention program of EPA RMP, enforced

[4]The term "process" means "any activity involving a highly hazardous chemical including using, storing, manufacturing, handling, or moving such chemicals at the site, or any combination of these activities. For purposes of this definition, any group of vessels that are interconnected, and separate vessels located in a way that could involve a highly hazardous chemical in a potential release, are considered a single process" [82].

[5]See Footnote 25 on page 10.

by the law, there are other (document-based) industry PSM frameworks. The CCPS model of process safety management encompasses: accountability, objectives and goals, process knowledge and documentation, capital project review and design procedures (for new or existing plants, expansions, and acquisitions), process risk management, management of change, process and equipment integrity, human factors, training and performance, incident investigation, standards, codes, and laws, audits and corrective actions, and enhancement of process safety knowledge. The Chemical Manufacturers Association Process Safety Management elements are: management leadership in process safety, process safety management of technology, process safety management of facilities, and managing personnel for process safety. The American Petroleum Institute Process Safety Management elements are: process safety information, process hazard analysis, management of change, operating procedures, safe[6] work practices, training, assurance of the quality and integrity of critical equipment, pre-startup safety review, emergency response and control, investigation of process-related incidents, and audit of process hazards management systems [9].

2.3 Other related work

2.3.1 Rasmussen's risk management framework

Rasmussen's risk management framework considers socio-technical systems with several actors, stressed by rapid technological change, a competitive environment, changing regulatory practices and public pressure. It suggests that risk management must be modeled by cross-disciplinary studies, and requires a system-oriented approach based on functional abstraction rather than structural decomposition [67].

[6]The term "safe" is commonly used, both in the industry and in the literature, and for that reason we preserve it in referenced texts; however, since risk can be decreased, mitigated, and managed, but it cannot be completely eliminated, we would rather use the term "safer" instead.

Rasmussen's framework, illustrated in Figure 2.3, has two components: a structural hierarchy that describes the individuals and organizations in a system, and the dynamic forces that can cause a complex socio-technical system to modify its structure and behavior over time [8]. The actors in this framework are depicted in levels: work, staff, management, company, regulators and associations, and government. The related research disciplines necessary for understanding risk factors vary at each level, and range from mechanical, chemical and electrical engineering; psychology, human factors, human-machine interaction; industrial engineering, management and organization; economics, decision theory, organizational sociology; to political science, law, economics and sociology. The environmental stressors encompass a fast pace of technological change, changing competency and levels of education, changing market conditions and financial pressure, and changing political climate and public awareness.

In order for the system to function adequately, vertical integration is required. Decisions must propagate top-down and information has to propagate bottom-up. The interdependencies across all the hierarchy levels are critical, making safety an emergent property. The lack of vertical integration, caused in part by a lack of feedback across levels, threatens safety, which implies that the decisions of all the actors, not just the front-line workers alone, can cause incidents. However, since nobody has a global view of the entire system, actors at each level cannot see how their decisions interact with those made by actors at other levels, so the threats to safety are not obvious before an incident occurs, and are usually caused by multiple contributing factors, not just a single catastrophic decision or action [8]. Rasmussen also remarks that "in this situation, modelling activity in terms of task sequences and errors is not very effective for understanding behavior" [67].

The second part of Rasmussen's framework considers financial pressures pushing the actors to work fiscally responsibly, and psychological pressures pushing the actors to work in a more mentally or physically efficient manner. As a result, work practices migrate over

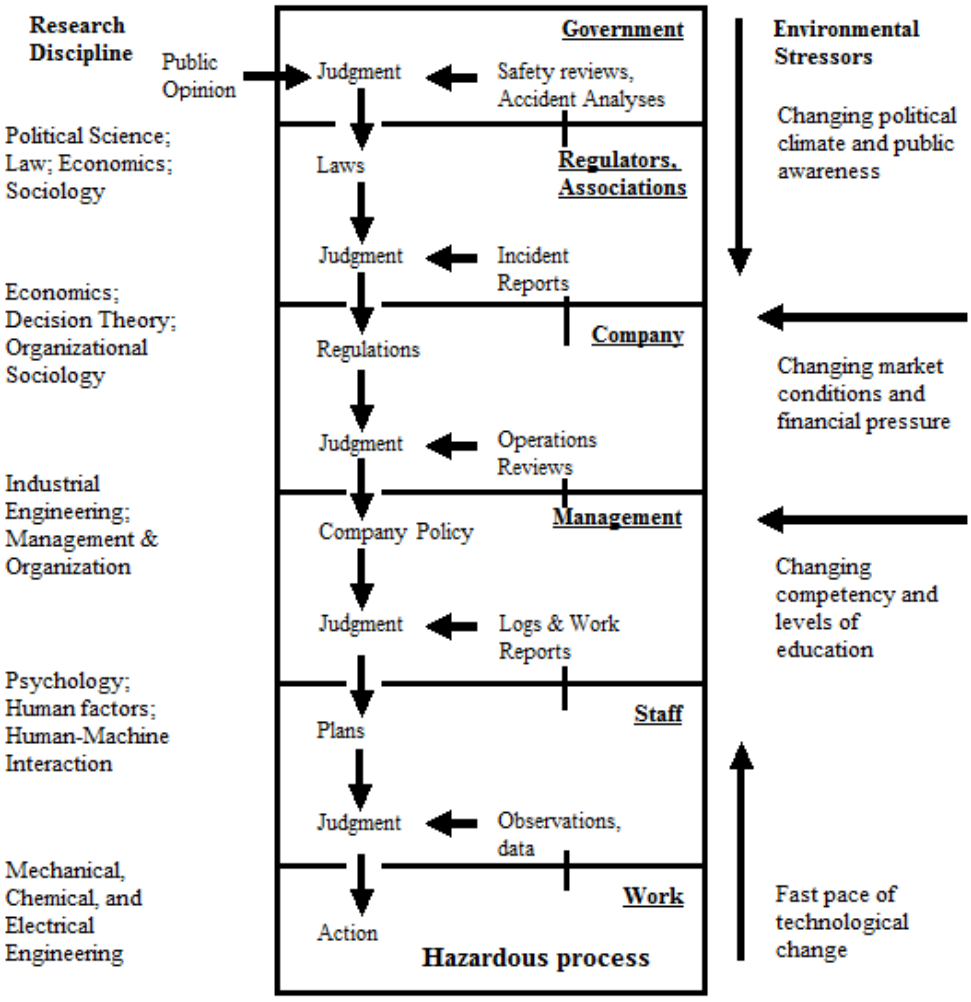

Figure 2.3: Rasmussen's risk management framework: the socio-technical system involved in risk management. Source: [67]

time, at multiple levels, toward the boundary of safety, making the systems defences degrade and gradually erode. After multiple migrations of work practices at various levels, and the presence of a triggering event, not just an unusual action or an entirely new, one-time threat to safety, incidents can occur [67], [8]. While the first part of Rasmussen's framework relates to the multiple stakeholders of protective systems, and their many interactions, the second part remarks the importance of MOC, not only in the physical com-

ponents of the system, affected by wear, technological changes, and financial constraints, but also in the people, practices, policies and procedures, as well as other intangible parts of the protective systems that can change over time, affecting its performance.

Rasmussen also developed the Accimap method as a means of graphically representing factors from different systems levels that have contributed to accidents[7]. Accimaps show the interactions between factors both within and across the different systems levels, and have been applied to the analysis of incidents within many domains [81].

2.3.2 HROs

HROs are those organizations that could have failed resulting in catastrophic consequences, and did not, in the order of tens of thousands of times. They are characterized by both advanced technology and high degrees of interdependence [70]. Common elements that HROs use to identify and mitigate risk are: effective process auditing, migrating decision making, recognition of goal conflicts, alignment of reward and punishment systems, redundancy of people and/or hardware in a variety of forms (including duplication and overlap), senior managers who can see the "big picture", formal rules and procedures, and lack of exclusive reliance on externally imposed rules and regulations [72]. Strategies to lessen dysfunctional characteristics in hazardous organizations include: continuous training, redundancy, responsibility and accountability at all levels in the organization, job design strategies to keep incompatible functions separate, have many direct information sources, flexible exercises, job specialization, system flexibility, hierarchical specialization, and bargaining and negotiation [69].

There are five major building blocks that are necessary for mitigating error, but that often seem absent in disasters: flexible organizational structuring, attention to reliability as a rival to efficiency, avoiding core competencies becoming incompetencies, adequate

[7] See Footnote 25 on page 10.

sense-making, and group performance and heedful interaction [71]. The incident command system (ICS) is an organizational approach to emergency or disaster management, able to attain remarkable reliability under a broad range of working conditions, including the uncertain and instable ones. Its components are: structuring mechanisms, organizational support for constrained improvisation, and cognition management methods [4].

2.3.3 Safety function

SysML has been employed successfully in the aerospace industry. Jensen and Tumer [42] recently used SysML to evaluate the safety of a system under critical event scenarios involving one or more component failures, in the early design stage of a maneuvering system for a satellite. They stated that when a failure in a system happens, it is the components, and not the functions, which behave differently. In their system model, besides the object view for the software and hardware components, and the view of function for their behavior, they added another view, defined as "safety functions", to describe the property of a system to resist moving from a hazardous state to an accident[8] state. When a system is in a hazardous state, it can only transition into the mishap state if the safety function is lost or ineffective, thus, they developed a method to represent the safety functions as part of the design process. Their safety functions are comparable to protective systems in a broad sense.

2.4 Literature review on specific topics covered in the introduction

2.4.1 Lack of historical data on failure of protective systems, consequences, and alternative sources

In the introduction we mentioned that the lack of historical data on the failure of pro-

[8] See Footnote 25 on page 10.

tective systems complicates analysis. Protective system failure is very infrequent. Near misses, however, are much more frequent. Models such as the safety pyramid, based on the work of H. W. Heinrich[9], illustrate the typical frequency of occurrence of incidents, and show a large difference in the ratio of serious incidents and near misses. According to them, for every fatality, there are about 30 serious injuries, 300 minor injuries, 3,000 near misses, and at least 300,000 at-risk behaviors. They suggest that the underlying causes of incidents at each level are essentially the same, and therefore more serious incidents can be reduced by focusing on the bottom of the pyramid, where more data exists. While it is a good idea to identify and address the initiating causes of incidents, it must be clear to the reader that, even in the presence of an initiating cause, if protective systems work as intended, the critical consequences can be prevented or mitigated. The information provided by the study of near misses may not always be related to aspects affecting protective systems, hence, its usefulness is limited.

2.4.2 Civil liability vs. safety regulation

In order to understand the role that regulators and judges play to mitigate moral hazard and induce preventive and protective measures, as well as identify their limitations in these matters, in the following paragraphs we will examine related literature pertaining mostly to environmental damages.

Accident[10] law seeks to deter the risk-creators and compensate the victims when an accident occurs. Safety regulation intervenes *ex ante* (before an accident occurs), and civil liability intervenes *ex post* (after an accident occurs). From an economics perspective, an optimal level of care for deterrence purposes minimizes the costs of both accident and accident avoidance, while an optimal rule for compensation purposes transfers the losses

[9] See [35] for the original work and [68] for the models that derived from or extended it.
[10] See Footnote 25 on page 10.

from the victim onto the risk-creator [3]. In a civil liability regime, the social costs of the accident are shifted to the tortfeasor [77]; therefore, each risk-creator determines his level of preventive measures based on his costs of care and the probability of being held liable in case of accident [7]. Regarding environmental damages, theoretically, tort law may provide optimal care at lower costs than regulation [38], as an *ex post* liability system not only provides compensation, but also induces investments in prevention [27], [6] in order to avoid lawsuits, while regulation needs to be enforced whether there is harm or not, whenever a standard is breached. Furthermore, in a regulatory regime, the state has to determine the optimal level of care for each risk-creator [48], which implies that regulators need to know the costs of care of each polluter and the consequences of each accident to achieve best practice through regulation [3].

Despite the convenience of its lower cost, civil liability alone is not the preferred tool, as it has three serious failures in the environmental risk domain [3]: the problem of rational apathy[11], the problem of causal uncertainty[12], and the problem of insolvency[13]. Broadly, in technological disasters, even when a liable tortfeasor can be identified, the damage must be directly attributed to causes that are man-made for liability rules to play their preventive and compensating functions. "The only possibility to apply tort law in case of natural disasters is to argue that public authorities were at fault e.g. by failing to prevent the disaster or not taking adequate measures to mitigate the damage" [27][14]. Although catastrophes caused by terrorism are man-made, the terrorist may not always be found or

[11] Victims may not sue when damages are widespread, as the damages every individual victim suffers are too small compared to the legal costs of suing, or simply because damages are unknown at the time they occur, as is the case in carcinogenic emissions. Rational apathy is treated in [59].

[12] Causal uncertainty refers to the difficulty to establish the causal link between damages and a polluter's activity with absolute certainty.

[13] Polluters may cause damages far higher than their assets. Insolvency occurs in any situation where the amount of the damage is higher than the tortfeasor's wealth, which is very likely to happen in case of catastrophes [27].

[14] For example, if the government failed to give proper warning in case of a flooding, or provided building permits on the slopes of an active volcano [27].

can be insolvent. Finally, in some cases private parties may lack adequate information on preventive technology, while the government can take advantage of economies of scale to invest more efficiently in preventive technologies and pass on information to the parties in the market through regulation [27]. Therefore, regulation is commonly accepted as a more effective instrument to control externalities[15] [78] and prevent environmental accidents [73], [23]. Economists favor the combination of safety regulation and insurance to cope with industrial accidents, particularly when environmental damages may occur [3].

Nevertheless, in practice, the deterrent effect of regulation often fails due to financial and informational constraints [65]. Financial constraints refer to the fact that the limited budget of regulatory agencies may impede an adequate level of monitoring or supervision of critical facilities; whereas informational constraints imply that "regulators have to determine the costs of abatement and the costs of care for each polluter, and this information is privately owned by polluters themselves" [3]. Also, certain aspects of safety are difficult to observe before an accident occurs, as they would require detailed knowledge of internal characteristics of every firm. This is the case of organizational negligence as a product of understaffing, which often leads to excessive working time, an inadequate delegation of power, or the lack of appropriate skills for certain jobs [3].

While both *ex post* civil liability and *ex ante* safety regulation have limitations, it has been demonstrated that the joint use of liability and regulation is socially beneficial [3], [27], [6], [75]. The activities of regulators and judges in promoting safer management of hazardous operations are complementary and interdependent. Judges often rely on prior regulation when dealing with cases of causal uncertainty, and use breaches of regulation as evidence of increased risk of an activity by the perpetrator. On the other hand, they do not accept the compliance with regulatory standards as a defense against liability. However, if, despite having complied with regulation, an accident still occurs, judges observe

[15] Such as damage to critical infrastructure.

the polluter's careful management and relieve him from civil liability only if he also took enough precaution in this dimension of care[16]. Judges can hold regulators liable when regulators did not monitor a regulated plant. Judges also dispute over the regulation itself (e.g. with conflicting national and regional regulations, or whenever ancient and new standards coexist). Furthermore, the problems raised by victims before courts help regulators identify the need to adapt norms and standards to current issues [3]. In practice, sharing information and coordinating actions among regulators and between judges and regulators is complex, among other reasons, due to the variety of local officials and polices with the same role [3].

Various studies show that the impact of monitoring and enforcement actions of regulators on the environmental performance of polluters has been positive [54], [50], [31], [61], [20]. However, as mentioned earlier, financial constraints may prevent regulatory agencies from performing these actions efficiently. When the measurement of emissions is very costly, regulators may attempt to infer a firm's compliance status based on the inspection of production and abatement equipment, the review of its production and environmental records, and interviews with its employees [55]. Conversely, when measuring emission levels is feasible, one way to complement or supplement traditional enforcement actions is the adoption of structured information programs (or public disclosure programs) to reveal the environmental performance of polluters [29]. It has been shown that public disclosure helps to induce emission reduction [46][17], with a relatively stronger impact than that of fines [29], and that the judgments of environmental performance that customers, suppliers and stockholders do affect the expected costs and revenues of some firms [18]. One of the reasons to support information disclosure as an enforcement tool is that stock markets re-

[16]In [75] the author proposes to sufficiently reward the injurer whenever an accident happens and socially optimal precaution has been taken.

[17]In [46] the authors found that firms with the largest stock price decline on the day their toxic release inventory (TRI) emissions information became public subsequently reduced emissions more than their industry peers.

act significantly to the release of information regarding the superior or poor environmental performance of plants [33], [46], [49]. This, in turn, is an incentive for the shareholders of the firms to demand management to invest in protective systems to prevent major releases of pollutants (or more broadly, any safety-critical incident), when companies are publicly-traded (which may not always be the case).

Besides shareholders, insurers, and other type of financers, e.g. secured lenders, may also induce the firms to adopt adequate prevention measures. This is because in some countries and under certain circumstances[18], in order to mitigate the insolvency problem, courts may "extend liability for residual damages to parties that have contractual relationships with the firm that causes the damages" [6]. Conditioning financing or insurance to the adoption or continuing use of existing protective systems, or transferring the expected liability costs financers would face to firms' financing conditions, may be strong incentives for companies to adopt best practices and invest in protective equipment. Even in the event an accident occurred and protective systems failed, this measure would be beneficial to the victims, who otherwise would not receive compensation and end up paying the costs if the tortfeasors were insolvent. In that case, the remaining costs would be shifted from the victims to the financers. Although the insolvent company or companies in which the incident originated[19] would still not cover all the damages, it can be argued that moral hazard would be reduced, as financers do profit from the operation of the company in more favorable circumstances, or have already recovered the costs through the premiums and interests charged. However, in reality, insurers and "financers have only incomplete

[18]For example, when the involvement of secured lenders in the firm, before and/or after the accident and/or the foreclosure, exceed the level warranted to secure their interest [6].

[19]These may include, in some cases, the designers or the manufacturers of the equipment that failed.

information about the preventive measures adopted by the firms they finance" [6][20].

The neighboring community is another agent who may interact with companies directly, but in most cases does it through either regulators, or non-governmental organizations, to demand information, law enforcement, and safety and environmental measures, which could be translated into the use of protective systems.

> Communities which are richer, better educated, and more organized find many ways of enforcing environmental norms. Where formal regulators are present, communities use the political process to influence the tightness of enforcement. Where formal regulators are absent or ineffective, 'informal regulation' may be implemented through community groups or NGOs (non-governmental organizations) [29].

Considering the effect that releasing information to the public can have in the behavior of the firms, as well as the existence of multiple agents able to induce various forms of safety and environmental practices in companies, and who need information in the process, it becomes clear that regulators can take advantage of informational approaches to enforce the law.

> Once we introduce a world of multiple agents (and consequently multiple incentives), there may be a need to rethink the regulator's appropriate role in pollution management. It may be that this role is no longer confined to designing, monitoring, and enforcing rules and standards. Instead, the regulator can gain leverage through non-traditional programs which harness the power of communities and markets. In this context, there may be ample room for

[20] Recall that the problem of asymmetry of information previously identified enables moral hazard. In the end, the intention of this work is not merely to make those who profit under favorable circumstances, or the responsible of causing a catastrophe pay the costs and compensate the victims, but to prevent catastrophes from occurring. Legal actions that enforce the adoption and use of protective systems are therefore of interest. We believe that, in order to design, manage, and regulate effective protective systems, asymmetry of information and moral hazard need to be addressed.

information-oriented approaches such as the public disclosure of plants' environmental performance [29].

In fact, the role of regulators is not limited to establishing, controlling, inspecting and enforcing regulation. Governments and regulators act as information clearinghouses who acquire information, synthesize it, and make it available to people who are making social choice decisions. By performing such activities, they contribute to decrease the asymmetry of information related to moral hazard. Some countries may have more or less communicative regulatory bodies than others; however, communication with the public is an essential duty of the regulatory authority, particularly in the context of safety[21].

[21] In the U.S. nuclear sector, for example, the International Atomic Energy Agency (IAEA), whose responsibilities include "providing independent, neutral, balanced and factual information about any issue related to nuclear safety in the country" [39], remarks the importance of having regular routine communications with its audiences, in addition to communicating in response to incidents; being notified of unusual events by their licensees and provide them with feedback on recent safety developments and inspections completed; communicate with decision makers, coordinating communication activities to provide coherent information when regulatory responsibilities for nuclear safety are divided among different organizations; communicating with regulatory counterparts in other countries; working with professional organizations, universities, NGOs, etc., to exchange information, increase awareness of their respective works, get acquainted with new developments, and understand and address their concerns. With regard to communication, its counterpart in Finland, the Radiation and Nuclear Safety Authority (STUK) is responsible for writing, publishing and distributing educational material and background information, organizing meetings with journalists and other interested groups, providing timely information on events related to nuclear safety, and responding to the questions of political decision makers, other government authorities, journalists, or members of the general public [39].

3. CONCEPTUAL MODEL OF PROTECTIVE SYSTEMS

This section presents our conceptual model of protective systems, depicted in Figure 3.1, and describes its elements, interactions, and dynamic nature.

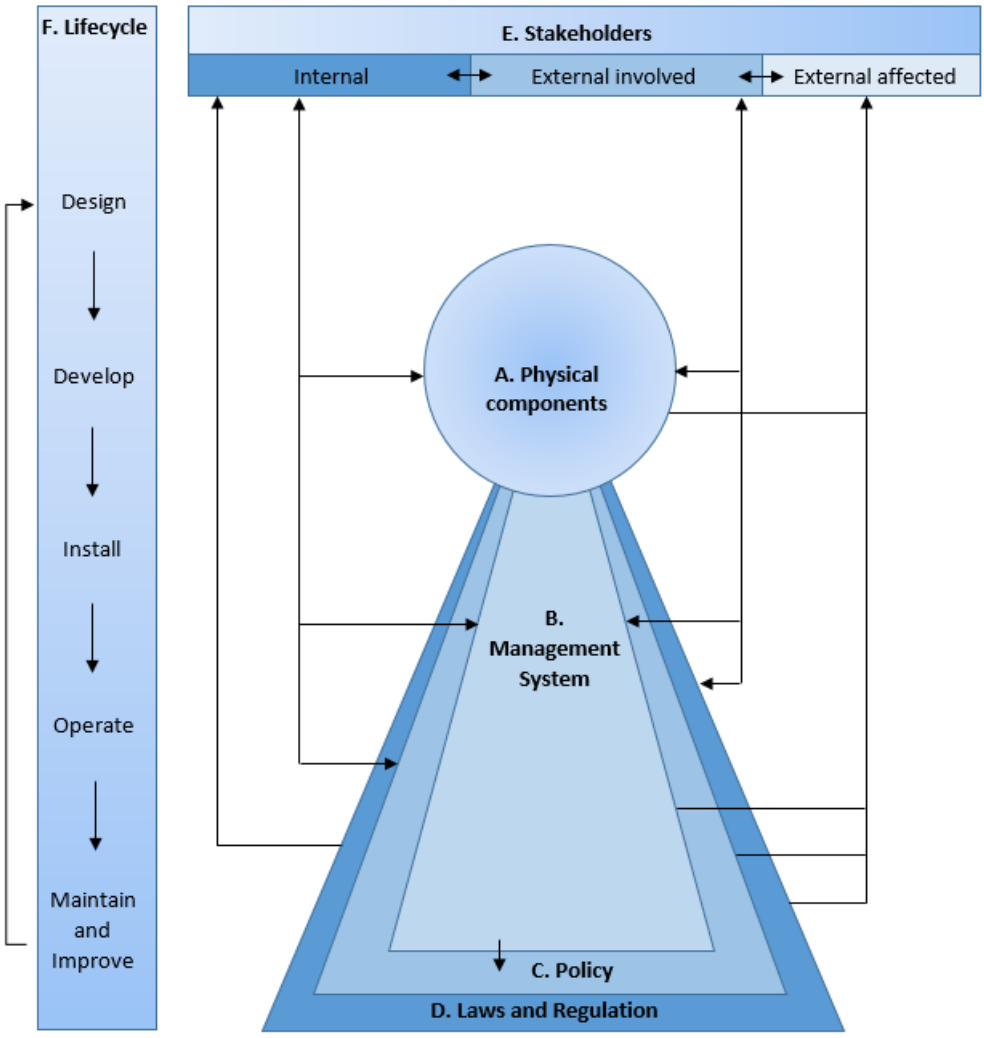

Figure 3.1: Conceptual model of protective systems.

Our conceptual model graphically represents the various broad, interrelated elements,

that together constitute a protective system. We identify the respective parts or instances of each element, in order to provide a baseline to derive the structure our system model (developed in section 4). Then, we discuss some of the interactions among these elements, as well as their dynamic nature. This stresses the importance of understanding them while managing protective systems, and serves to recognize further structural aspects, as well as some of the behaviors and requirements that our system model should encompass.

3.1 Elements for the structural decomposition

3.1.1 Physical components

We begin with the physical components (A), such as those in the preventive, mitigative, barriers, and limitation layers of protection. Examples of these components include sensors, alarms, pressure relief devices, dikes, water curtains, and emergency shutdown systems.

3.1.2 Management system

The physical components are supported by a management system (B), which comprises the structure, processes and resources included in the inherently safer design, control and supervisory layers[1], as well as the management part behind the response layer. The management system is an essential part of any protective system. It includes the operating procedures, control systems, monitoring and supervision activities during regular operations to prevent hazardous events and correct anomalies.

The management system encompasses several activities of major importance: design procedures, management of change, documentation, hazard assessment, processes intended to review and preserve equipment integrity, human factors, training, audits, inci-

[1]Recall the protection layers in Figure 2.2.

dent investigation, and emergency response, among others. A detailed list of the process safety management elements related to management systems can be based on standards and models such as those presented in section 2.2.2.

3.1.3 Policy, laws and regulation

The management system involves the structure, processes and resources needed to establish the operating policy (C) of the protective system. This policy must comply with the applicable laws and regulation (D).

3.1.4 Stakeholders

The conceptual model also captures the existence and role of the stakeholders (E). They can be classified into three broad groups: the internal ones, who belong to the company and are actively involved in the design, operation and management activities (e.g. management, workers); the external ones who do not belong to the company but are also involved in such activities (e.g. manufacturers, first responders, regulatory authorities); and the external who are not actively involved but can be affected when the protective system fails (e.g. near neighbors).

3.1.5 Lifecycle

The lifecycle (F) suggests that there are various stages that depend on and build upon each other over time. The artifacts of our system model should illustrate that certain activities occur only during specific stages. They should also show that the outputs of each stage may become the inputs for the subsequent, inheriting further characteristics, consequences of decisions or issues to address. While decommission and obsolescence may happen, this model focuses on evolution and continuous improvement, consistent with a "cradle-to-cradle" philosophy.

3.2 Interactions and dynamics: requirements and further structural and behavioral features to capture in our system model

Our conceptual model presents a brief structural decomposition of the main types of elements of a protective system. Indeed, protective systems are more than their physical components, which are designed, developed, installed, operated, maintained, and improved, until they are decommissioned due to their obsolescence, and replaced by better technology. By definition, the protection layers are supported by a management system, in which various stakeholders who own and operate, or are affected by them, define and execute the internal operating policy, or the laws and regulations that must be complied, and all these activities occur in various stages of the system lifecycle. However, although all these broad elements are necessary for the system to function, the interactions within and among these elements, as well as their dynamic nature, are of major importance. As such, they need to be understood and included in our system model.

3.2.1 The importance of understanding the interactions among elements

Clearly, physical components interact among themselves. Final elements will only work when logic solvers determine that based on the inputs provided through the sensors; closing a valve on the discharge of a pump may result in pump damage; or opening a pressure control vent valve could affect the amount of released gases that flares or incinerators will need to burn. In a similar fashion, there exist several interactions among the elements of a management system. Lessons to learn revealed in audits and incident investigations, as well as new operating procedures, have to be communicated to the appropriate personnel and contractors in the form of training; hazard analysis or evaluation need process safety information, and changes in any element have to be assessed and approved by management of change. For the sake of simplicity, this conceptual model does not show all possible interactions among elements of the same type; however, it illustrates

some important interactions and dependencies.

The arrows that connect each lifecycle stage represent how stages depend on and build upon each other. Other artifacts of the systems model should show what stakeholders participate in each stage. The needs of the three groups of stakeholders are refined into requirements for the physical components and the management system that supports them. Internal stakeholders can determine the policy, while some external stakeholders can affect the applicable laws and regulation. Stakeholders, therefore, can affect the physical components, the management system, the policy, and the laws and regulation that comprise the protective system, but they are also affected when the protective system fails. Thus, our model connects these elements with bidirectional arrows.

Stakeholders also interact among themselves and may affect each other. The internal stakeholders, as well as the external involved, own the protective system and work together to design and operate it; therefore, they possess more information about it, compared to the remaining external stakeholders. However, the interests of these external affected stakeholders can be taken into account by some of the external stakeholders who are involved, including the regulatory authorities and some citizen participation groups who represent the near neighbors. As these two sets of external stakeholders interact, the issues that arise with asymmetry of information can be prevented or mitigated.

The management system (B), which is supporting the physical components (A) in our conceptual model, involves the structure, processes and resources needed to establish the operating policy of the protective system. The arrow that connects the management system and the policy is intended to illustrate this unidirectional dependency. The policy must comply with the applicable laws and regulation (D). The model does not include an arrow that connects the policy with laws and regulations because the policy does not automatically change when the regulation does. However, laws and regulation can affect the internal stakeholders who are able to change it directly, and the stakeholders who

create or modify the laws and regulations can affect the management system that helps to establish the operating policy. Graphically representing the management system (B), the policy (C), and the laws and regulation (D) as various layers with laws and regulation as the outer layer reinforces the idea of compliance.

3.2.2 The importance of understanding their dynamic nature

The elements of protective systems interact among themselves. These interactions need to be understood, as no individual has full visibility of the whole complex system, and yet, changes in one element can affect others as well. Nevertheless, changes are constant; protective systems have a dynamic nature. The safety-critical technologies they are intended to protect evolve over time, and protective systems must respond to the new demands as well. Their physical components become obsolete as they wear out and technology advances; personnel turnover stresses the importance of documentation and training, laws and regulations are amended, the needs and requirements of each type of stakeholders change, and the operating policy suffers modifications as the management system adjusts accordingly. Change is inevitable and needs to be managed effectively, otherwise the efficacy of protective systems can be compromised. For that reason, MOC is essential.

We have identified the elements of protective systems and some of their essential features, and have remarked the importance of understanding their interactions and their dynamic nature. The concepts analyzed have provided us with an idea of the structure and behaviors to include in a system model, created according to the tenors of MBSE, which will be presented in the next section.

4. RESULTS

In this section we develop a new model[1] of protective systems, and demonstrate some of the capabilities and benefits of using the MBSE approach to address their challenges. The complete diagrams mentioned in this section can be found as appendices, in the separate file *Diagrams.pdf*.

4.1 SysML model

4.1.1 SysML model of protective systems

In the previous section we described a conceptual model of protective systems, which included the physical components, the management system that supports them and helps to determine the operating policy, consistent with the applicable laws and regulations, in which various stakeholders participated throughout its various lifecycle stages. Based on that broad representation, we have crafted a model in SysML that allows us to present in detail each one of those elements, including their structure, their behaviors, and more importantly, the relations and interactions among them.

This model has over 500 blocks, 74 activities, 49 packages, 31 requirements, 77 use cases, and 7 views and viewpoints, depicted in over 65 diagrams, which were created with information extracted and adapted from texts such as the CCPS guidelines [13], [10], [14], and OSHA PSM [82].

4.1.1.1 LOPA as simply one of many views

The reader must be aware that the diagrams in SysML are views of the systems model,

[1] We used the modeling language SysML, and the software NoMagic MagicDraw 18.3 with its SysML Plugin.

which reveal portions of the model at specific levels of granularity. Under this logic, the current characterization of protective systems as a group of protection layers used in LOPA, commonly utilized in the industry, can be included in our model as one of its many views. Later, we enhance this characterization by integrating the elements from our conceptual model. A detailed view of the protection layers serves as a starting point to capture the physical components. Figure 4.1 depicts the types of protection layers and initiating causes.

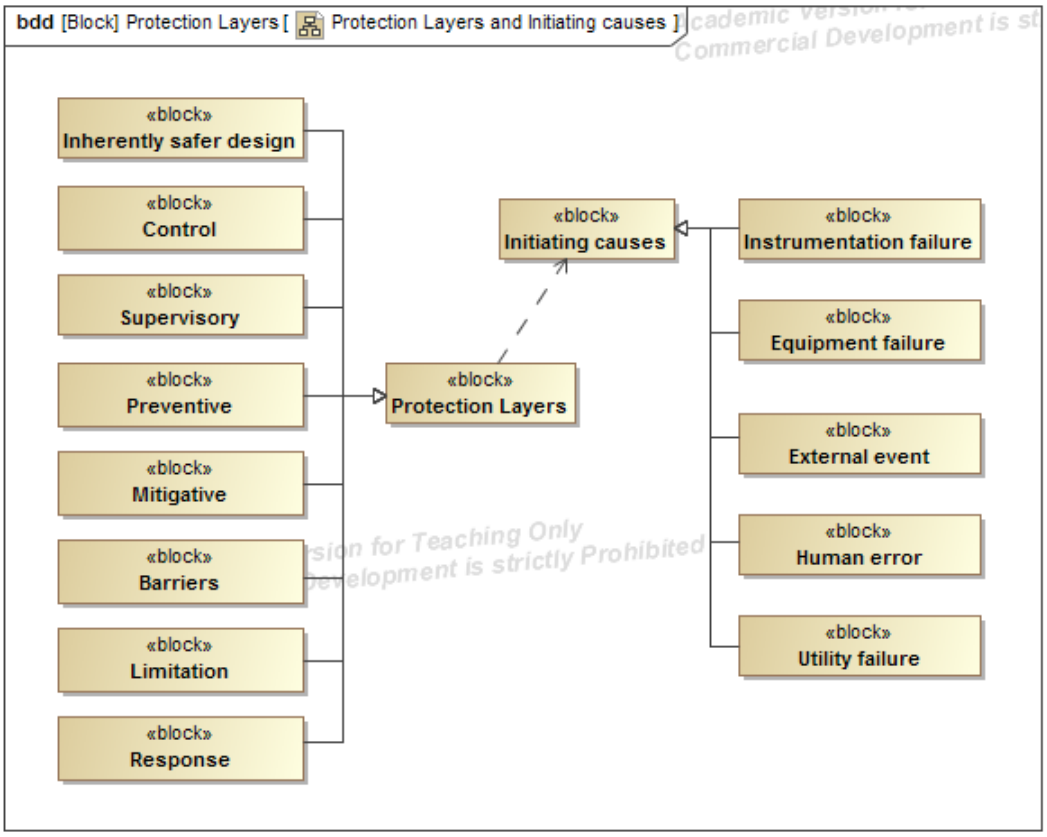

Figure 4.1: Protection layers and initiating causes.

Diagram 1 shows a taxonomy[2] of the protection layers. It displays the generalization[3] between some devices and the type of protection layer into which they can be classified. Complementing this diagram, Diagram 2 has a taxonomy of initiating causes. A more detailed view of the protection layers in Diagram 3 contains not only generalizations but also composite associations[4], reference associations[5], and dependencies[6].

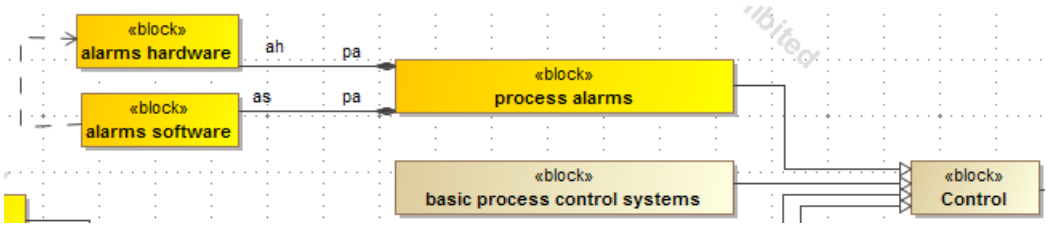

Figure 4.2: Portion of BDD in Diagram 3 depicting process alarms.

A portion of Diagram 3 is shown in Figure 4.2. It illustrates that process alarms belong to the Control protection layer, that they have hardware and software, and that changes to alarms hardware may affect alarms software. Another portion, shown in Figure 4.3, includes pressure relief devices, knockout drums, condensers, incinerators, scrubbers, vents and two kinds of flares (ground and elevated). It exposes the unidirectional connections

[2]The type of diagram used here to convey system decomposition and type classification is a block definition diagram (BDD).

[3]The notation for a generalization is a solid line with a hollow, triangular arrowhead on the end of the supertype [22]. It shows that the subtype is a type of a supertype.

[4]A composite association between two blocks conveys structural decomposition. An instance of the block at the composite end is made up some number of instances of the block at the part end. The notation for a composite association on a BDD is a solid line between two blocks with a solid diamond on the composite end [22]. A composition denotes a class as an aggregate and describes a whole-part hierarchy. The aggregate is existentially responsible for its parts [89].

[5]A reference association between two blocks means that a connection can exist between instances of those blocks in an operational system, and those instances can access each other for some purpose across the connection. A solid line between two blocks with an open arrowhead on one end conveys unidirectional access, and the absence of arrowheads on either end conveys bidirectional access [22].

[6]A dependency conveys that when the supplier element changes, the client element may also have to change. The notation is a dashed line with an open arrowhead, which is drawn from the client to the supplier [22].

that exist among pressure relief devices with knockout drums, condensers and incinerators; pressure relief devices and vents; scrubbers and vents; and scrubbers and flares. It also shows that the necessary height of the elevated flares depends on the flare stack diameter, the distance from the flare base, the desired heat intensity, the vapor rate, and the molecular weight of the vapor. Diagram 4 reveals the functions that these types of mechanical equipment perform in a relief system.

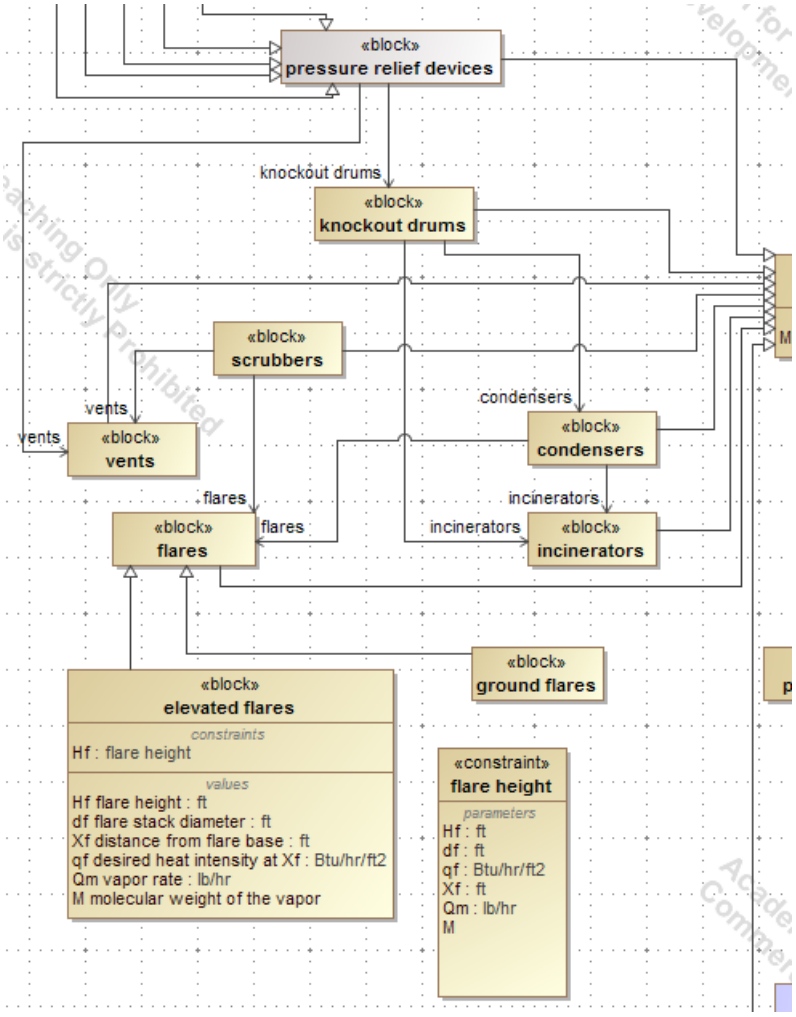

Figure 4.3: Portion of BDD in Diagram 3 depicting relations among various types of mechanical equipment.

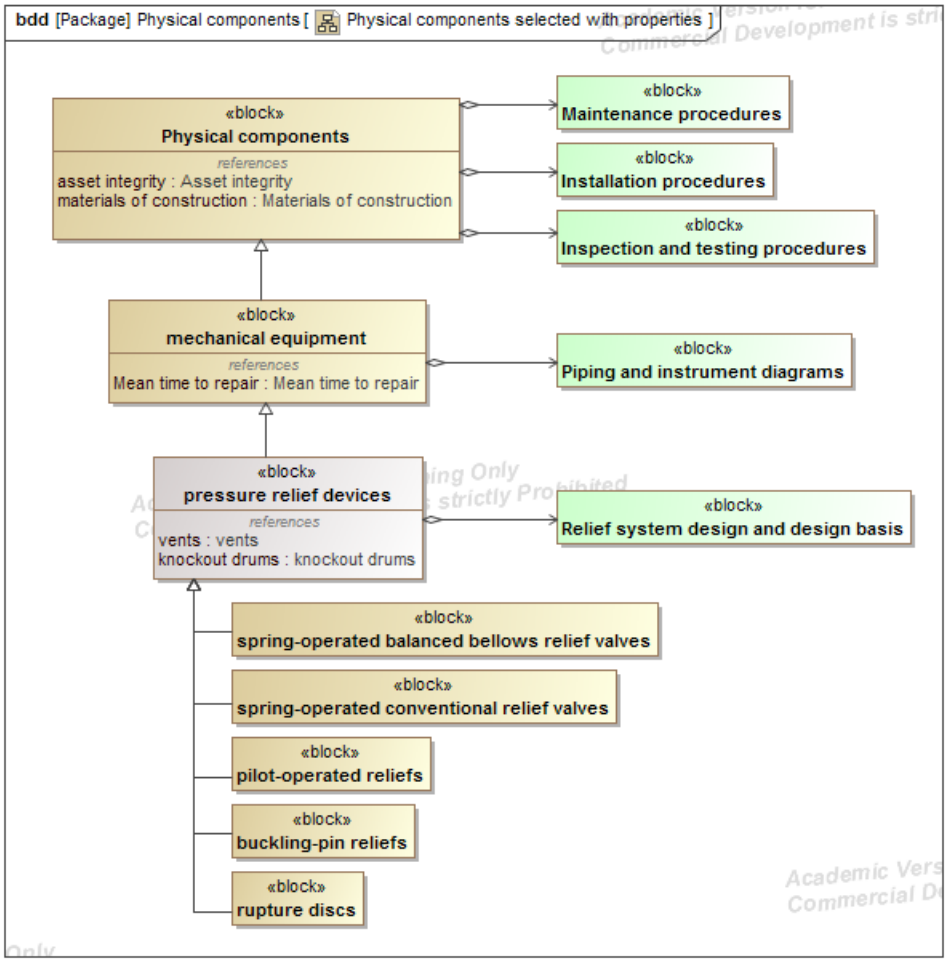

Figure 4.4: Selected physical components with properties assigned at various levels.

4.1.1.2 Physical components

Another view of the taxonomy of protection layers establishes, through generalizations, that most of the elements that constitute the protection layers are in fact physical components. This allows us to include the *physical components* from our conceptual model in our systems model, but it also gives us the possibility to assign structural and behavioral features to the block of physical components, which will be inherited automatically, by transitivity, to all the subtypes, and then assign further properties only to specific

subtypes.

This way, it is easy to state, as illustrated in Figure 4.4, that all physical components have maintenance procedures, installation procedures, and inspection and testing procedures; but only certain physical components have further properties, such as the mechanical equipment, which also has piping and instrument diagrams; while the various types of pressure relief devices, which are a subset of the mechanical equipment, have a relief system design and design basis as well. Diagram 5 presents the view of all the physical components of our model.

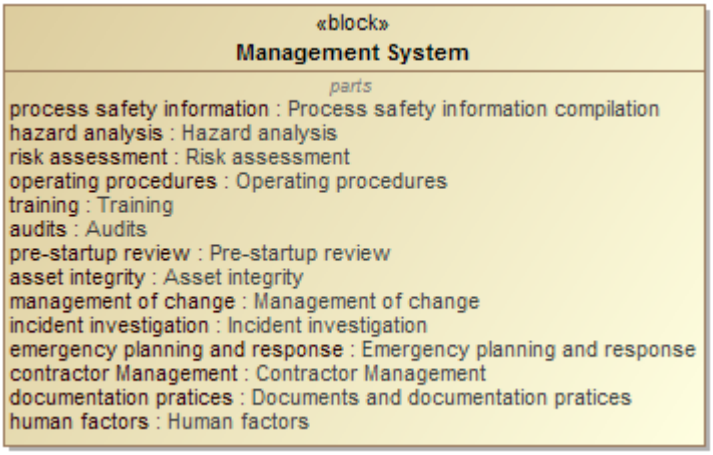

Figure 4.5: Block of the management system.

4.1.1.3 Management system

The *management system* is represented in our system model through several BDDs that display its various elements, including those present in OSHA PSM and some others from the models described in section 2.2.3, and their respective components, modeled as parts. The BDD in Diagram 6 shows them succinctly, and Diagrams 7 through 20 present the

BDDs of each individual element with their respective parts. Figure 4.5 exhibits the block that corresponds to the management system, with its elements displayed as part properties.

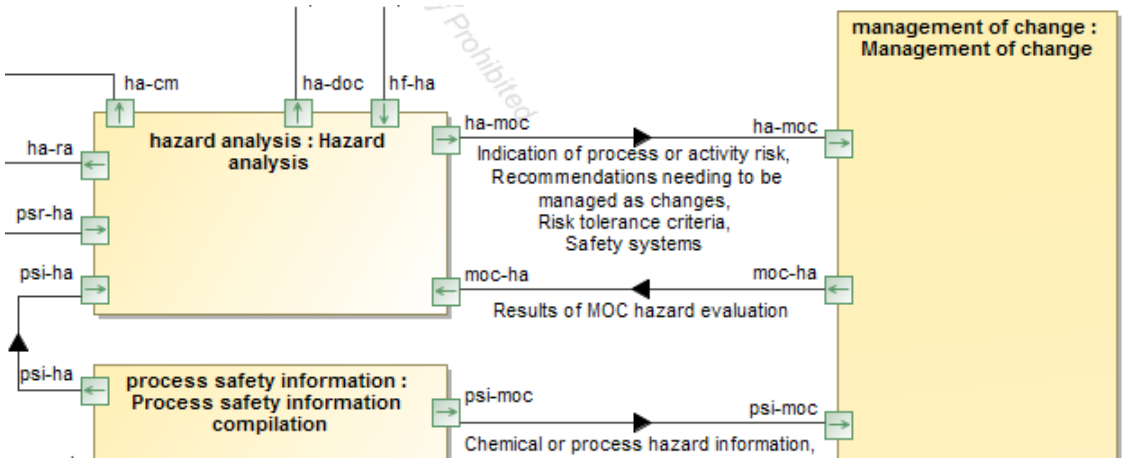

Figure 4.6: Portion of the IBD in Diagram 21 depicting information flow within the management system.

The internal block diagram (IBD) in Diagram 21 reveals the information and objects that flow across the parts (elements) of the management system, and therefore, possible interactions among themselves. It emphasizes the relevance of MOC, as several other parts of the management system interact with it. A portion of it is shown in Figure 4.6.

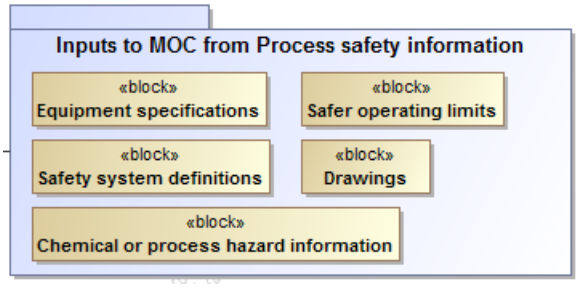

Figure 4.7: Package of inputs to MOC from process safety information.

The inputs and outputs to and from MOC are contained in various packages[7] displayed in Diagram 22. Figure 4.7 shows one of them. A similar diagram also reveals dependencies among the inputs and outputs, and the areas of the management system that could affect or be affected if they were modified.

4.1.1.4 MOC system

Given the importance of MOC, besides treating it only as a part of the management system, our model includes a section related to MOC systems, based on the CCPS guidelines in [14]. The commitment that is required from the management stakeholders to MOC involves the allocation of resources, the inclusion of MOC in the management system, and providing training to those who are involved in activities derived from or affected by changes. This is illustrated in Diagram 23. The key principles and essential features of MOC are shown as use cases in Diagram 24. The activity diagram in Diagram 25 allocates specific activities associated to them. These activities are not connected to each other by control or object flows because none of them are mandatory and in some cases can be executed concurrently. Prior to the formal execution of MOC, there are various tasks that should be performed during the design and development lifecycle stages to create a MOC system. They are stated in Diagram 26, which can also be used for comparison purposes, as these tasks are interrelated. The parts of the design specification are illustrated in Diagram 27, and then Diagram 28 depicts what it is implied in the development of a MOC system.

Diagram 29 analyzes the diverse roles in a team for purposes, summarizes the major functions of each role[8], and illustrates what internal stakeholders should play them. A very small portion diagram 29 is shown in Figure 4.8. It displays the block that corresponds

[7]The notation for a package is a folder symbol, that is, a rectangle with a tab on the upper-left side [22].
[8]Such roles are presented as use cases in Diagram 29.

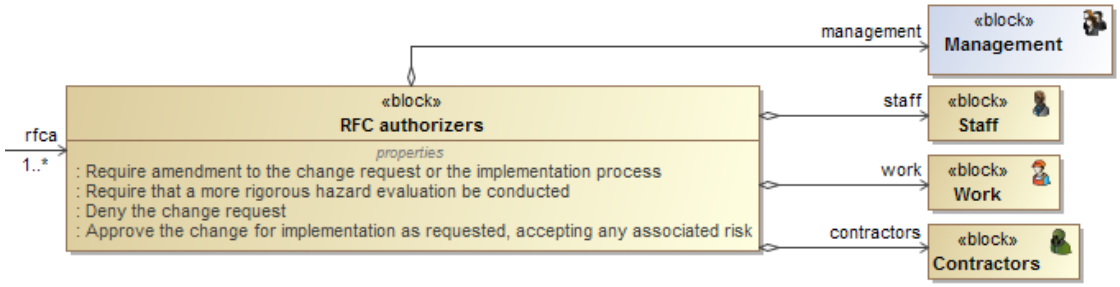

Figure 4.8: Portion of the BDD in Diagram 29.

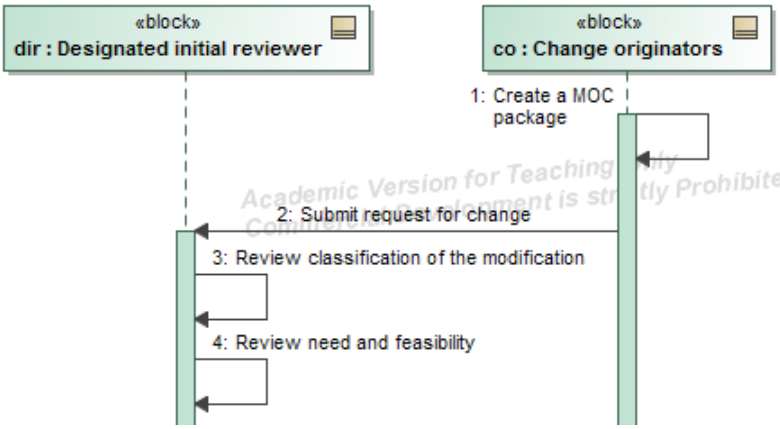

Figure 4.9: Portion of the SEQ in Diagram 31.

to the role of request for change (RFC) authorizers. The properties of this block state four possible courses of action that they are responsible for: require amendment to the change request or the implementation process, require that a more rigorous hazard evaluation be conducted, deny the change request, or approve the change for implementation as requested, accepting any associated risk. It also shows that personnel from management, staff, work, or contractors, may assume this role. Diagram 31 is a sequence diagram that shows the steps followed during management of change, as well as the interactions among the people playing each role. Figure 4.9 shows a portion of it. The activity diagram in Diagram 32 depicts the RFC review and approval procedure. A portion of it is shown in

Figure 4.10.

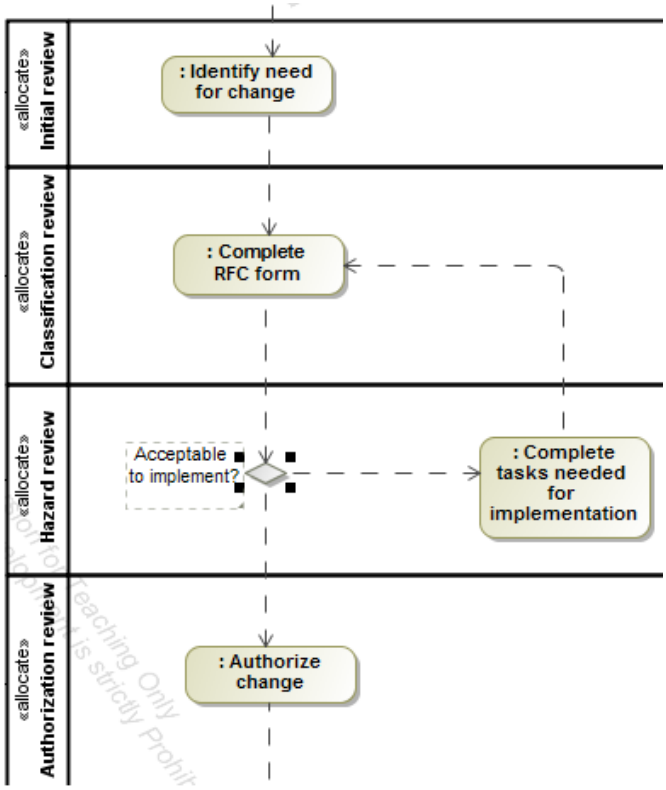

Figure 4.10: Portion of the ACT in Diagram 32.

4.1.1.5 Policy, laws and regulation

In this model, there are various ways to include the *policy* element from our conceptual model. One of them is through the above mentioned information that flows across the management system parts, as it includes procedures (e.g. maintenance procedures, inspection procedures) and criteria (e.g. risk tolerance criteria, criteria for applying procedures). Also, the operating procedures part from the management system itself[9] encompasses sev-

[9]See Diagram 16.

eral aspects of policy, from the steps required to correct or avoid deviation in the operating limits or the engineering controls and administrative controls in safer work practices, to the failure responses, compensating measures and procedures to apply when a shutdown fails, among others. Some blocks from the taxonomy of the protection layers in Diagram 1 are elements of policy as well. Another way to represent policy consists of the use of requirements[10]. Requirements can be written and organized in tables as in Diagram 33, depicted as part of block diagrams, or as requirement diagrams. Finally, another way to include the policy in the system model consists of the use of use cases and activity diagrams, to illustrate various courses of action[11]. Figure 4.11 exemplifies how to include policy in the diagrams using requirements and use cases. Diagram 34 shows one way to group various elements of policy.

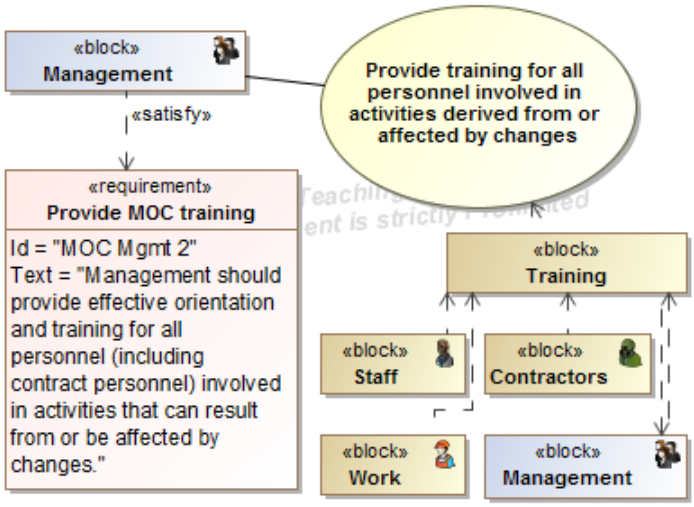

Figure 4.11: Policy depicted with a requirement and a use case.

[10]The notation for a requirement is a rectangle with the stereotype "requirement" preceding the name. Requirements have an id and a user defined text of type string. The relationships that can be created among the requirements and other model elements are: *containment, trace, derive requirement, refine, satisfy,* and *verify* [22].

[11]We will talk about use cases and activity diagrams later in this section.

The *laws and regulation* element from our conceptual model may be represented in blocks. It can be included in our systems model in the form of requirements as well, as shown in Diagrams 35 and 36, and indirectly, through the government and regulators, which are modeled as stakeholders. Also, we used requirements to model the core attributes of the protection layers in Diagram 37.

4.1.1.6 Lifecycle

Our system model presents various views regarding the *lifecycle*. The simplest one is in the form of a BDD, shown in Diagram 38 and Figure 4.12, which declares that the lifecycle is an aggregate[12] of various stages. The direct reference associations that link them convey the idea that they depend on and build upon each other[13].

SysML allows us to model the structure, but also the behavior of the system. The activity diagram shown in Diagram 39 illustrates the major broad activities that are supposed to occur during the different stages of the system lifecycle. Although our model does not encompass them, it is possible to create further diagrams that explain in greater detail each one of the activities shown, including other behaviors such as state machines or additional activities that can be invoked if enabled. The lifecycle stages appear as partitions in the form of swimlanes, and each activity is allocated to the stage in which it should be performed. The necessary inputs and outputs of each activity are depicted, as well as the flow of object tokens (in this case, information) and control tokens that enable the subsequent activities. A small portion of the activity diagram in Diagram 39 is shown in Figure 4.13. It depicts the activity "Develop instrumented protective system design basis that implements

[12] Aggregation describes a class as an aggregate and specifies a whole-part relationship between the aggregate (whole) and a component part. In contrast to a composition, the aggregate is not responsible for its parts [89]. The notation for aggregation is a solid line between two blocks with a hollow diamond on the aggregate end. A direct aggregation will have an open arrowhead on the part end.

[13] Although the position of the arrowheads in the direct reference associations between lifecycle stages might seem counterintuitive, the arrowheads do not stand for the chronological flow of information. Instead, their position suggest that later stages can access (information from) earlier stages.

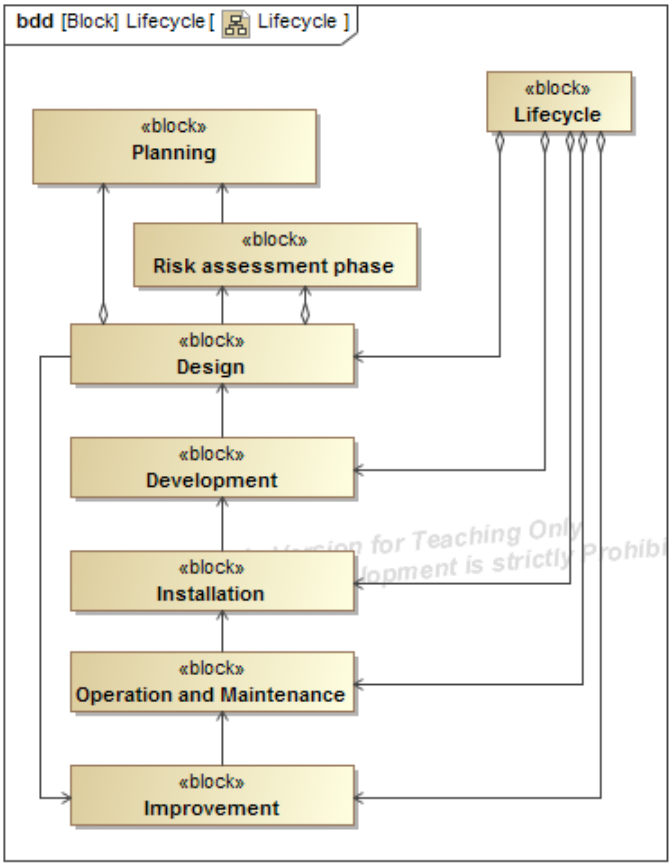

Figure 4.12: Lifecycle.

the risk reduction strategy" (the activity "Develop risk reduction strategy", not shown in the figure, precedes it), which is allocated to the design phase.

As opposed to the case of a simple drawing, in this model the inputs and outputs of the major activities performed during the lifecycle of a protective system are not just texts; instead, they are referenced to objects in the form of blocks that reside in a specific repository within the model and may appear in other diagrams. Therefore, they have properties (including parts and references) and further capabilities that are of interest for analysis, as well as in the management of protective systems and the management of change. For example, the first output of the activity depicted in Figure 4.13, corresponds to the block

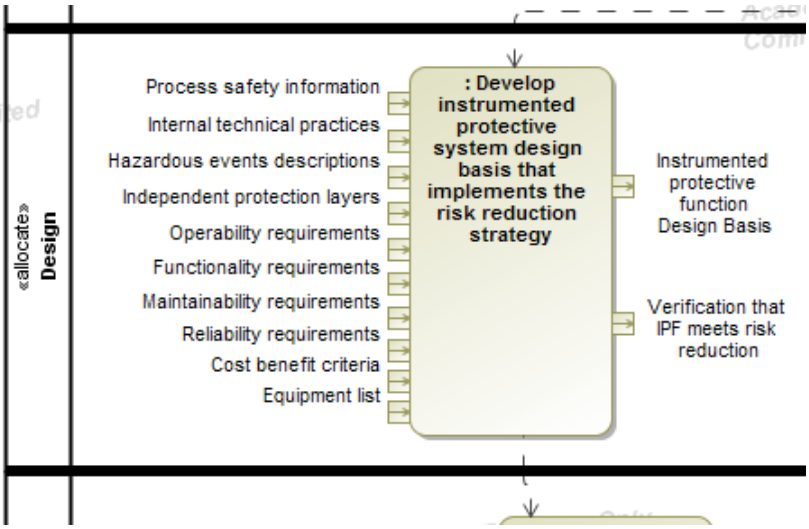

Figure 4.13: Portion of Diagram 39 depicting an activity within the design stage.

shown in Figure 4.14. The reference properties it contains summarize other blocks it aggregates, which in turn have more direct aggregations.

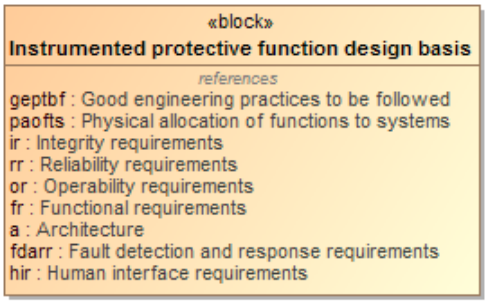

Figure 4.14: Block of the instrumented protective function design basis

Some elements are inputs to more than one activity throughout the lifecycle stages, others are outputs from one activity and inputs to another. These repetitions may be difficult to identify in this activity diagram. However, other diagrams reveal them with more clarity, and also include the structural decomposition of these elements. The BDD in Dia-

gram 40 shows the structure of the elements, organized according to the lifecycle stages to which they are allocated, i.e., where they are used (placing emphasis on which elements are used during each lifecycle stage), and color coded to specify whether the block corresponds to a lifecycle phase, an input, an output, an input and output, or a requirement. A portion of its miniature can be found in Figure 4.15.

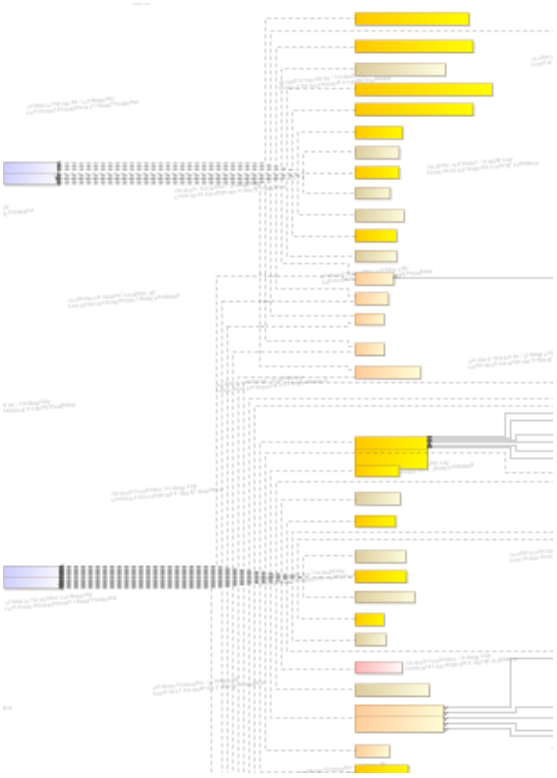

Figure 4.15: Miniature of a portion of Diagram 40 showing that the blocks of some inputs and outputs are allocated to more than one lifecycle stage (blue).

Diagram 41, whose miniature is shown in Figure 4.16, presents the same content, but rearranged as a tulip (placing emphasis on the elements and in which stages they are used). The blocks at the core are used in various lifecycle stages, while those in the periphery are used during one stage only. Therefore, the elements at the core may have a

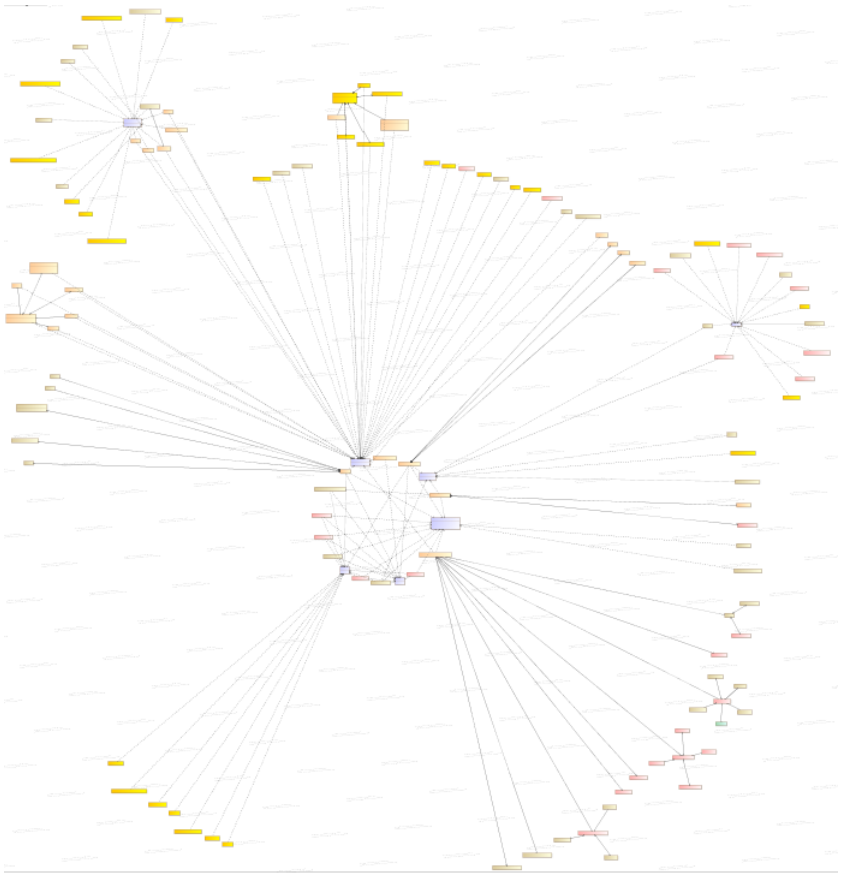

Figure 4.16: Miniature of Diagram 41 with inputs and outputs arranged as a tulip.

greater importance and complexity in the whole system. These are[14]: hazardous events descriptions (4), independent protection layers (2 plus a dependency), instrumented protective function design basis (2), operability requirements (3), process safety information (4), reliability requirements (3), internal technical practices (3), functionality requirements (3), maintainability requirements (3), independent protection layers analysis report (2 plus a dependency), equipment list (4), and detailed engineering specification (2).

[14]The number between parentheses next to them corresponds to the number of allocations to lifecycle stages that they have.

4.1.1.7 Stakeholders

There are various diagrams in our model that include the *stakeholders*. The BDD in Diagram 42 presents a basic classification of the three main groups of stakeholders considered in the conceptual model, and broad categories of representative people or groups within them. Although the software tool we used allowed us to show them as icons, they still are blocks, and can have the properties and functionalities that blocks do. A portion of this diagram is displayed in Figure 4.17. Diagram 43 shows a more detailed taxonomy of stakeholders, which encompasses stakeholders considered in various mismatching CCPS guidelines, but also in Rasmussen's framework, and those explicitly mentioned in OSHA PSM. The use of generalizations in the diagram allow the subtypes to inherit the properties assigned to their supertype.

Although every stakeholder contributes to or is affected by the protective system efficacy at some point, not all the stakeholders participate in each lifecycle stage. Furthermore, the roles and concerns of those who participate in more than one stage vary accordingly. Diagram 44 summarizes the stakeholders that actively participate in each lifecycle phase and their respective concerns[15].

Similar to Figure 4.18, Diagrams 45a and 45b contain the views[16] and viewpoints[17] with the various concerns of those stakeholders during the stages in which they participate. Furthermore, they include packages that contain all the elements of the model allocated or somehow associated to such lifecycle phases, detailed in Diagrams 46 through 52. This allows to compartmentalize the model and grant that the stakeholders have access to only

[15] Based on [13].

[16] A view is a package that selectively imports other packages, elements, and diagrams in the system model that together represent an aspect of the model that is of interest to a particular set of stakeholders [22].

[17] A viewpoint is a model element that contains the stakeholders (those that would find this viewpoint relevant to their concerns), the concerns (a string that expresses the stakeholder questions that will be answered by the elements and diagrams contained within a conforming view), the purpose (a string that specifies the reason why the viewpoint was defined), the languages (a list of the modeling languages used in a conforming view) and the methods (the set of rules followed to construct a conforming view).

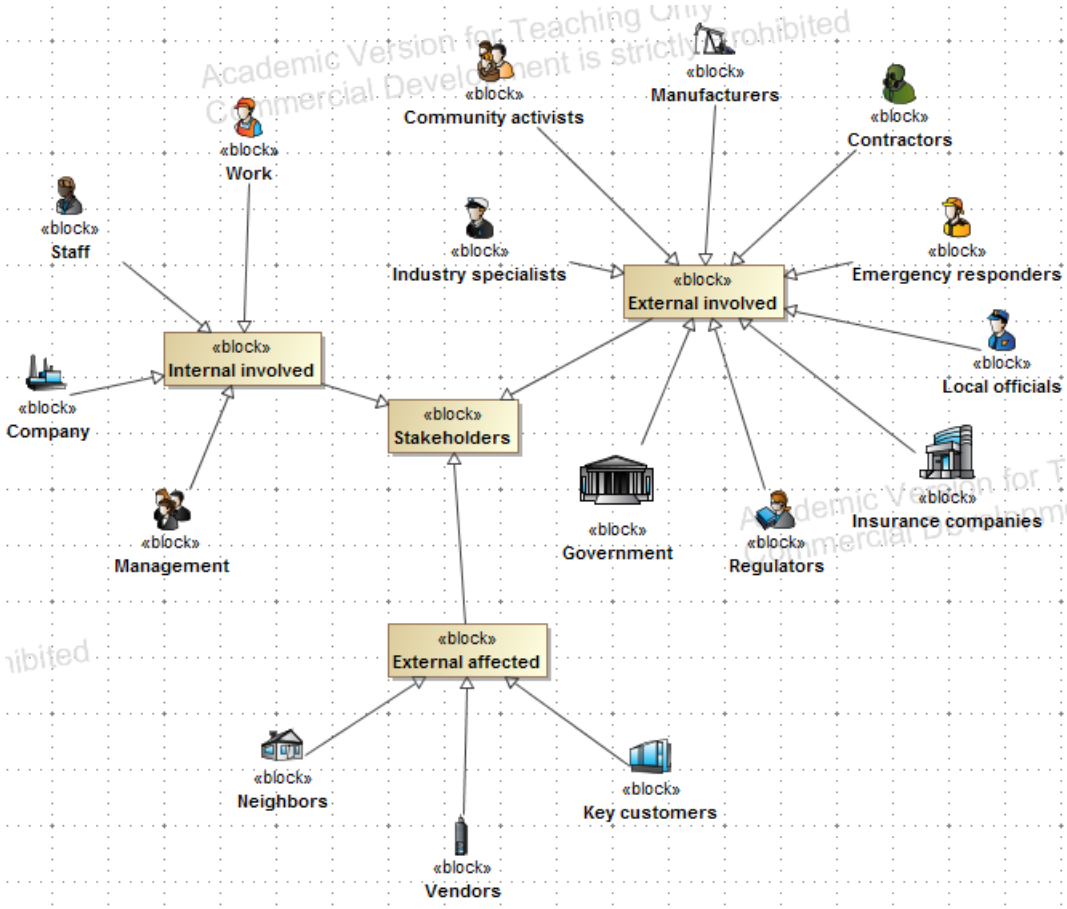

Figure 4.17: Stakeholders.

the model elements that are relevant to them, or to those they are authorized to see. While this makes sense in terms of security and specialization, the limited visibility of the stakeholders and the impact their actions and decisions could have in other parts of the system by this practice stresses the need to have tools to overcome it.

4.2 Analyses yielded by MBSE

MBSE allows us to employ various software tools that work with SysML, and provide managers (or other users) with tools for impact analysis and management of change.

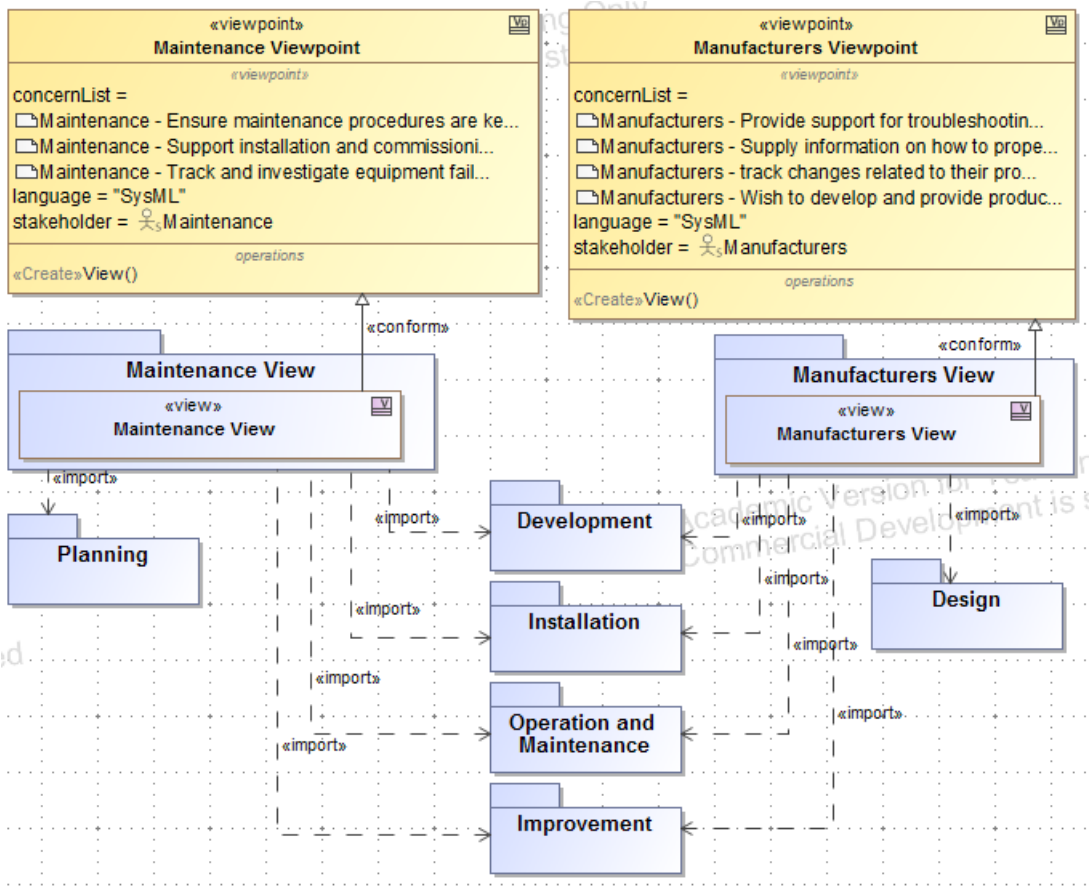

Figure 4.18: Views and viewpoints of two stakeholders importing packages.

4.2.1 Identify where a model element is used

Suppose we wanted to make a change in one of our model elements. In order to determine whether that would impact other parts of the system or not, we would need to know where else in the model that element is used. The software tool we have chosen to create our model of protective systems has the capability to quickly identify in which diagrams that object appears, open them, and show its location, or navigate through them.

4.2.2 Identify the relations among elements

Knowing the usage of an element in other diagrams is convenient, but it is not enough

to view that element in isolation. As we have previously suggested, there exist several kinds of relations among the model elements. Therefore, we need to identify the other model elements that interact with it, as well as the types of relations it has with them. We can quickly display in the current diagram the related elements from other diagrams[18], or display a list with the elements of the model that use it or depend on it.

Alternatively, we can generate a dependency report[19], which will list all the model elements that have any kind of declared relation with the element, as well as the type of relation, such as containment, dependency, allocation, association or direct association, aggregation or direct aggregation, composition or direct composition, generalization, applied stereotypes (including imports of packages) or if it is a connector though which information is conveyed from one node to another. Nevertheless, the dependency report has some limitations: it does not show the direction of the arrows in the relations (i.e. it does not specify whether the related element is a client or a supplier), and it does not display inherited relationships (i.e., those assigned to a supertype). Both can be overcome by opening the specification of block properties directly in the software for the desired blocks.

Another option we have is to generate a dependency matrix[20], or an allocation matrix[21], which will display all the elements in the model in the first row and column vectors and the existing relations among them in the appropriate entries[22]. Of course, in models with several unrelated elements these matrices are very sparse. A portion of an allocation matrix is shown in Figure 4.19. Either the dependency report or the dependency matrix can be used to identify further possible impacts. If the model only declares a dependency between

[18]The software will modify a diagram in which the element appears, by displaying its related elements and the type of relation they have.

[19]In Microsoft Word.

[20]In Microsoft Excel.

[21]In MagicDraw

[22]These matrices have the same limitations a dependency report has. Thus, using the specification of block properties in conjunction with the matrices is recommended.

elements A and B, and between elements B and C, the user of these reports may be able to infer that element C could be indirectly affected by element A; thus having the big picture that dependency matrices provide could be beneficial.

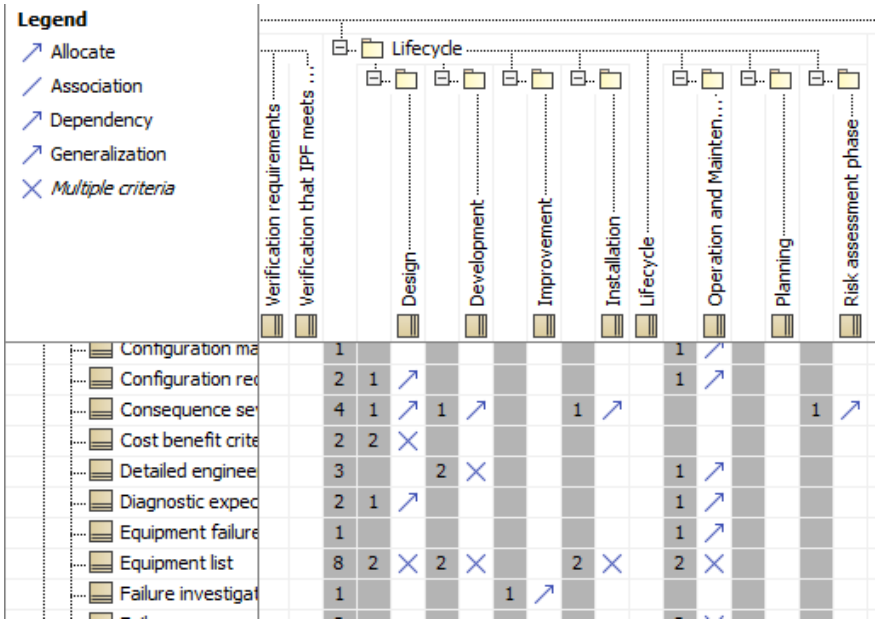

Figure 4.19: Portion of an allocation matrix.

Needless to say, these capabilities are limited or of very little use when the relations between elements are not modeled. However, in a well constructed model, they can be very useful for impact analysis and management of change.

4.2.3 Impact analysis, in the context of management of change, requires a model and a method

One of the key principles and essential features of management of change is to evaluate

possible impacts[23]. The outputs of our model, and our model itself, offer the stakeholders tools to perform this activity, as impact analysis requires a model and a method.

We have presented a detailed model[24] of protective systems that includes several interrelated elements displayed in its various views. Its outputs include lists and matrices that show the dependencies and other relations among its elements, and the software functions allow the user to quickly identify where each elements is used. Therefore, our proposed method for impact analysis recommends to first use the tools to identify where an element of the model is used, in order to ensure that a possible change to it that seems pertinent according to a diagram, is indeed suitable in the remaining diagrams. Second, the user should refer to the outputs of the model and check what are the other elements that have any dependencies or other declared relations with the element whose impact is being analyzed, and what kind of relations exist among them. If there are dependencies[25] with other elements, the user should go further and identify the dependencies that those related elements have with other not already considered elements.

4.2.4 Simulation

Our model also offers quantitative capabilities, and is suitable for simulation and other subordinate analyses, including trade studies and LOPA. We modeled various equations used in LOPA[26] in constraint blocks, and defined value properties[27] in some blocks that

[23] According to the CCPS, the key principles and essential features of management of change are: (1) Maintain a dependable management of change practice, (2) Identify potential change situations, (3) Evaluate possible impacts, (4) Decide whether to allow the change, and (5) Complete follow-up activities [14].

[24] This model can be extended and adapted to the characteristics of the industry in which will be used.

[25] Dependencies communicate that a change in the supplier element (at the arrowhead end) may result in a change to the client element(at the tail end). Therefore, the user must pay attention to the direction of the dependency to determine whether the element is a client or a supplier.

[26] The equations are variations (according to its various steps) of the equation used to compute the mitigated consequence frequency for a specific consequence, for an initiating event. See Section 2.2 for more detail.

[27] Including the probability of failure on demand, the number of similar layers, and the frequency of the initiating event.

refer to two particular types of layers of protection and an initiating event (See Diagram 53 or Figure 4.20).

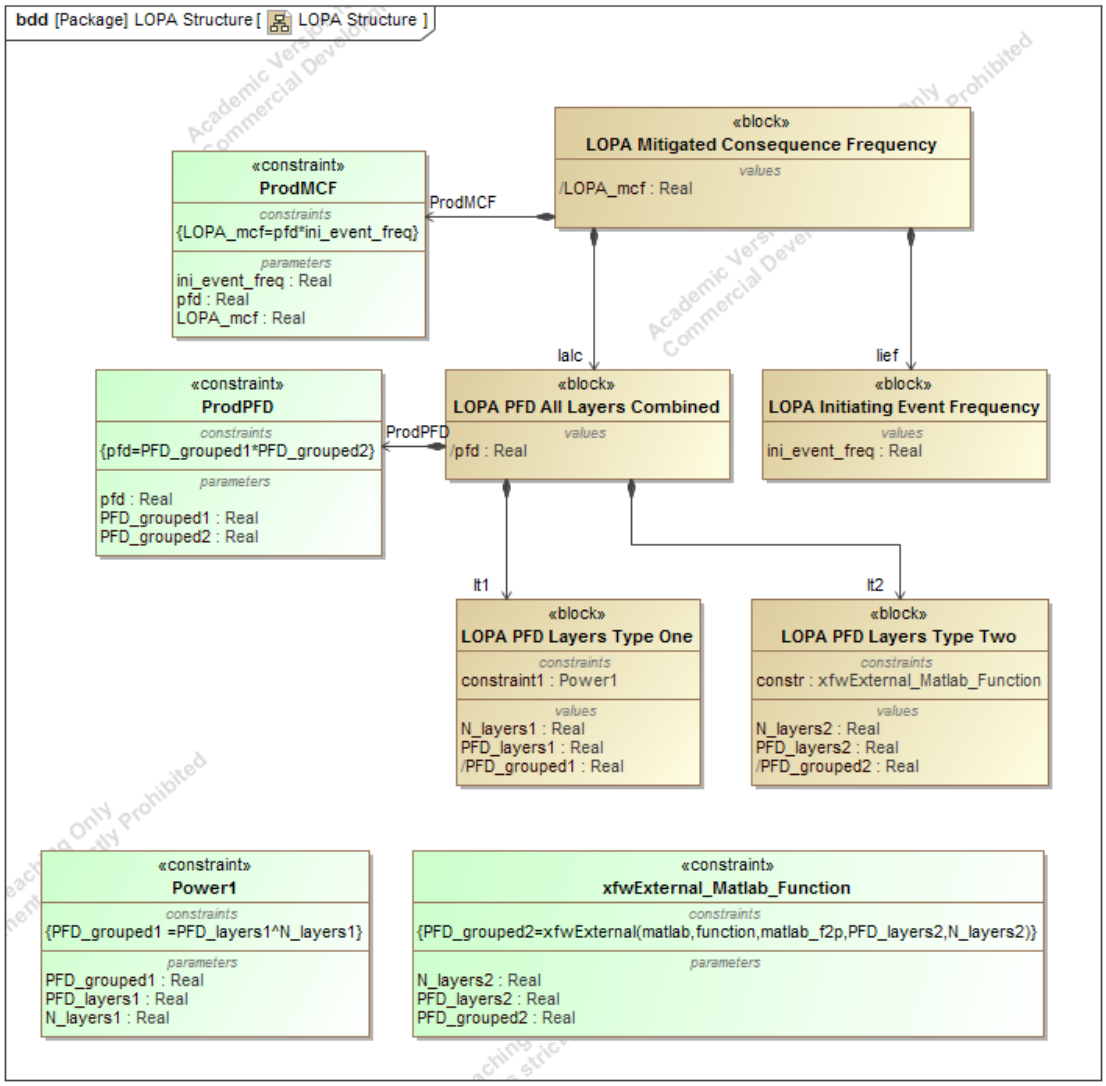

Figure 4.20: LOPA structure for simulation.

Then, we sketched various parametric diagrams to display the bindings between the variables in the equations and the value properties of such blocks (See Diagram 54 or

Figure 4.21).

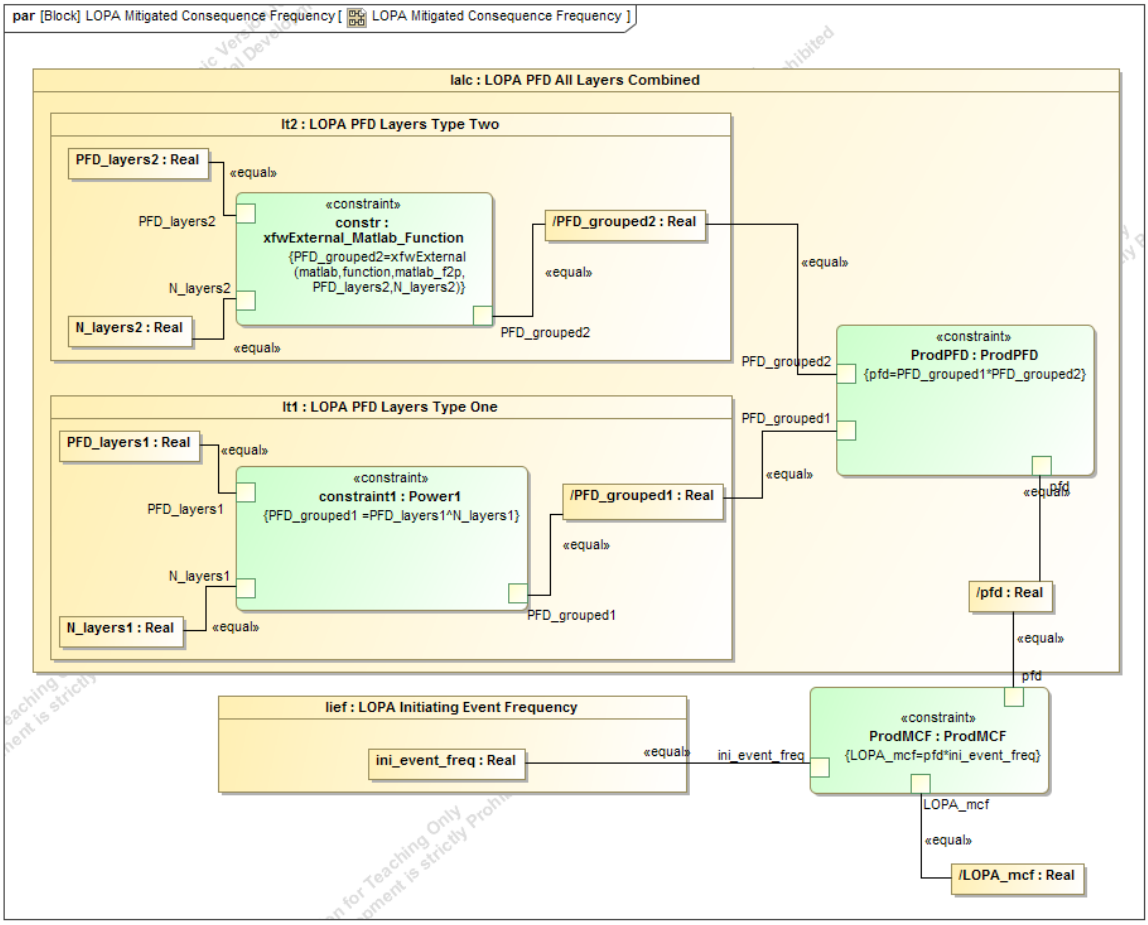

Figure 4.21: Parametric diagram of LOPA for simulation.

After that, we created instances for the blocks, as those in Diagram 55 or Figure 4.22, where the user can input values either manually, or importing them from a Microsoft Excel spreadsheet. The software uses an interface[28] to use either MathWorks MATLAB or Wolfram Mathematica as the core solver where the computations are performed, and then returns the target value(s). It allows the user to update the input and target values in the

[28]The ParaMagic Plugin developed by InterCAX LLC.

SysML diagram where the instances are depicted, as well as in the spreadsheet, if desired, provided that the necessary setup has been done.

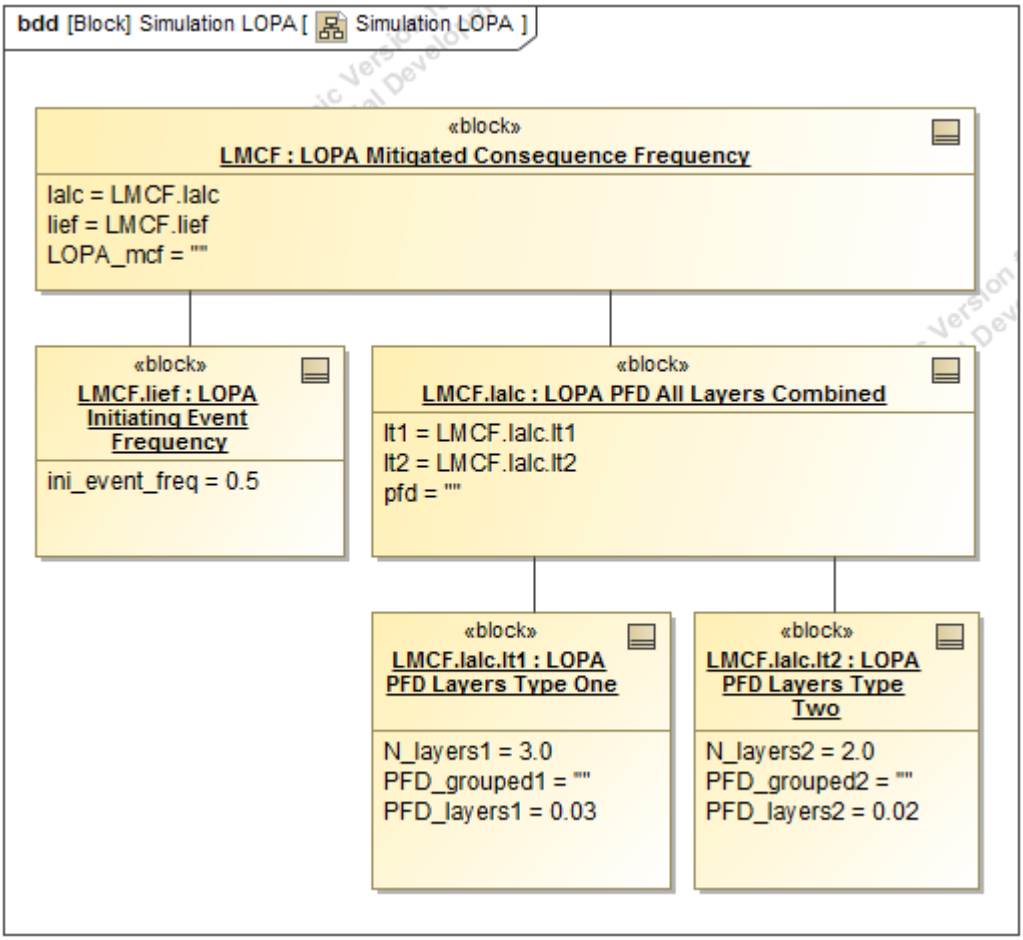

Figure 4.22: Instances of LOPA for simulation.

Although there exist certain limitations, the constraint blocks can also include user-defined functions and scripts to be run in MATLAB or Mathematica during the simulation, which creates the possibility for both deterministic and stochastic approaches. Also, by being able to import from Excel the values to populate the instances, the users may also take advantage of other software tools that work in combination with Excel, such as Pal-

isade's @risk. Trade studies, on the other hand, are only supported with Mathematica as core solver, and one or more Excel spreadsheets with the input variables for the desired number of scenarios to evaluate.

4.2.5 Animation to find deadlocks in activity diagrams

MBSE offers tools to improve processes that can affect the efficacy of protective systems. The UML/SysML activity diagrams depict the flow of objects through activities and nodes, and control tokens that enable actions[29]. They express the order in which actions are performed, and (optionally) which structure performs each action.

Although their shapes are different, the elements in activity diagrams have the equivalent functions of the places, transitions, arcs, and tokens of Petri nets[30]. A Petri net is a mathematical modeling language that can be used to describe concurrent, stepwise processes in discrete systems. Petri nets are used in safety instrumented systems reliability analysis and testing strategies, as described in [52], but they can also be used to model several other processes in the context of emergency response and safety in general. A deadlock is a set of places such that every transition which outputs to one of the places in the deadlock also inputs from one of these places [88]. The detection of deadlocks in a process during its design is very important, as they could make it stop and prevent it to function as intended. Finding deadlocks informally[31] in a diagram can be difficult

[29] Actions start when the activity that owns the action is currently executed, a control token arrives on each of the incoming control flows, and a sufficient number of object tokens arrive on each of the incoming object flows to satisfy the lower multiplicity of the respective input pin [22].

[30] In [26] the authors conclude that the main difference between the Petri net semantics and the semantics of UML activity diagrams is that Petri net semantics models resource usage of closed, active systems that are non-reactive, whereas the semantics of UML activity diagrams models open, reactive systems. If a Petri net is used to model a reactive system, the reactivity of that system is abstracted away from. Given that reactivity is considered one of the most important aspects of workflow modelling, activity diagrams may constitute an even better alternative in some cases. Reactivity can be simulated to some extent in Petri nets by modelling the environment in the Petri net as well.

[31] There exist various formal methods that require solving logical equations or solving systems of linear equations or inequalities in order to detect deadlocks.

and time consuming, however, the animation capabilities in the activity diagrams of our computerized model allow us to find them more easily than in a static Petri net or activity diagram.

4.3 How some practices from high reliability organizations are or can be embedded in the model

SysML allows to embed in our protective systems model some practices from HROs. The use of *redundancy*[32] can be forced by modeling the element that we want to be redundant, whether it represents hardware or people, as a part of another block[33], or using composite associations to convey structural decomposition[34], and establishing in the part properties or the parts end a multiplicity of 2 or more instances of an item, instead of the default multiplicity of 1, or the unconstrained number of instances when the multiplicity is set as 0..* or *.

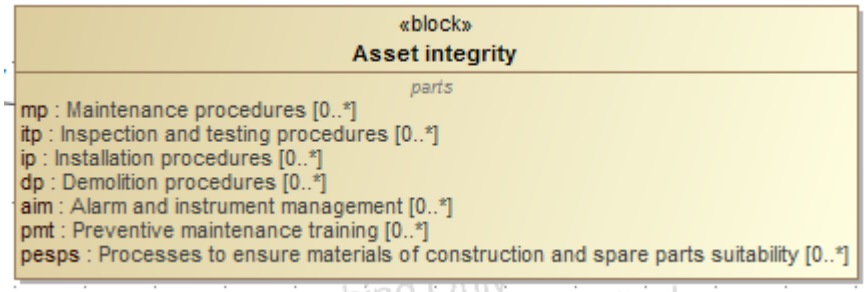

Figure 4.23: Parts of the asset integrity block where the notation for the multiplicity is visible.

[32] Which is often necessary in order to have independence in protection layers.

[33] As the part properties of the Asset integrity block in the Management System BDD in Diagram 6 or Figure 4.23.

[34] As those in Diagram 7 or Figure 4.24.

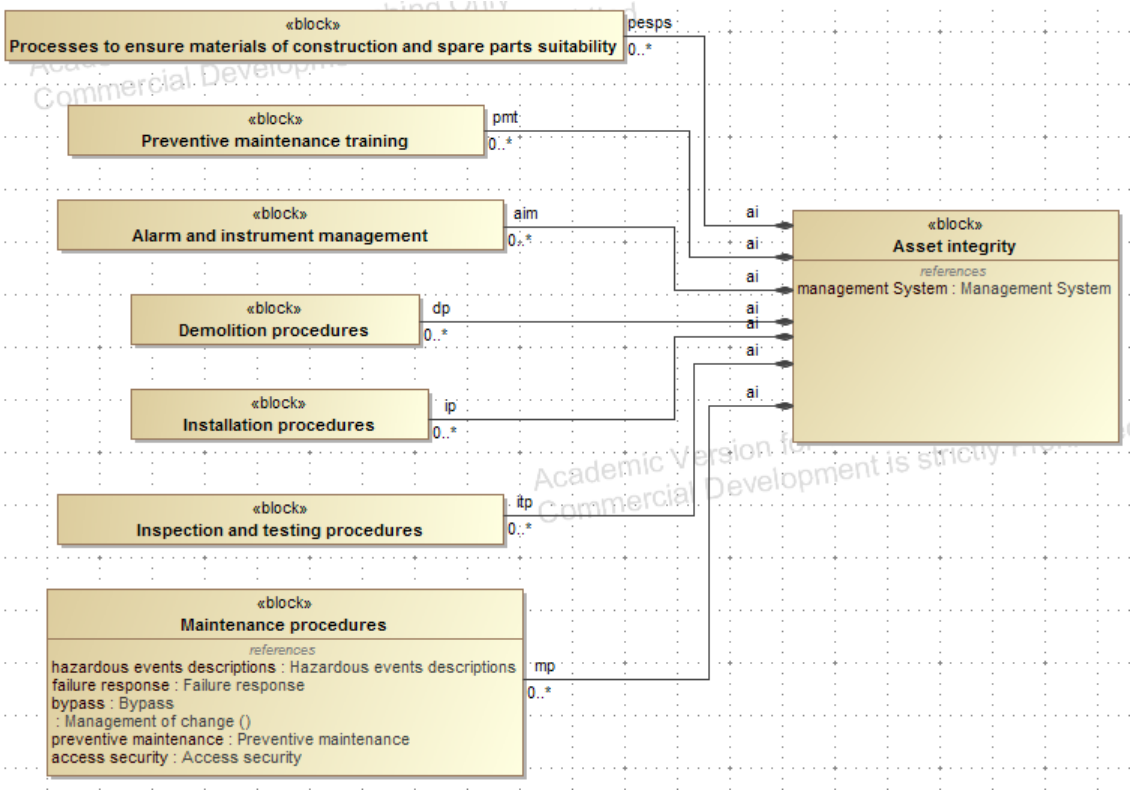

Figure 4.24: Composite associations of the asset integrity block

Formal rules can be modeled as requirements, as long as they include the satisfy and the verify relationships, to allocate such requirements to a structure, and a test case, which is a behavior created for the purpose of invoking a particular structure's functionality to verify that it satisfies the requirements allocated to it. *Procedures* can and should be modeled using behavioral diagrams, such as the activity, sequence, and state machine diagrams. *Training* and *audits* must be included in the management system. *Hierarchical specialization* may be modeled in BDD with the use of generalizations, focusing on the characteristics of the subtypes. Of course, simply including these features in our model does not automatically make protective systems highly reliable, but it helps to establish characteristics that the protective systems should or must have to maintain or increase

their reliability.

4.4 Implications of having cross-sections, views and viewpoints, in the context of shared governance and multiple stakeholders

Many of the model elements evolve around the lifecycle stages. The activities performed, their inputs and outputs, the stakeholders who participate in each one of them and even their respective interests and responsibilities vary across the stages. For that reason, it is useful to have packages or subsets of the model that contain specifically the model elements that are applicable during each stage. This way, each stage can be explained and be part of a model library, that later can be shared with the stakeholders involved, or be imported by another model that encompasses further issues related to that time frame. However, in order to understand and address better the concerns of each one of the stakeholders, regardless of the number of lifecycle stages where they participate, it may be convenient to have a subset of the model that contains the parts that are relevant for them. Partitioning the model and presenting it as cross-sections is possible with the use of packages or package diagrams. These views will filter the model according to the aspect intended to address, or the point of view of the stakeholder in question.

This cross-sectional modeling style, together with the capability of the modeling language to handle and show many views and viewpoints, is very useful in the context of shared governance and multiple stakeholders. It can help to clarify the roles and responsibilities of each group, or to understand the needs of other groups, and therefore identify possible gaps. A single view of the elements that more than one type of stakeholders have in common can be created, to facilitate collaboration. It can also allow external stakeholders to obtain the information about the protective system that they need to know without gaining access to restricted aspects of the company that it should not disclose, such as classified information, confidential business information, and trade secrets.

4.5 Advantages and drawbacks of having a computerized model, for maintenance purposes, instead of a set of disjoint artifacts

The MBSE approach has many advantages over its document-based counterpart with regard to maintenance. The artifacts in the document-based approach are a set of disjoint manuals, spreadsheets and other text-based files that need to be updated every time the system changes. It is very difficult to keep track of all the places in which the element that needs modification appears, and it is expensive and time consuming to ensure that all of the documents are properly updated. Any misses lead to inconsistencies among the updated and outdated artifacts, which makes the latter obsolete.

Our model of protective systems was constructed following the MBSE approach. Any changes made to an element of the model are automatically propagated to each and every place where that element appears, which makes maintenance fast, easy and inexpensive, and prevents inconsistencies caused by leaving one or more artifacts outdated by mistake. However, this advantage also has its drawbacks. Changing an element of the model based solely on one of the diagrams where it appears can be very dangerous, as it will instantly modify all the other diagrams in which the element to update is present, where the change may not always be desirable or perhaps even compatible, or could have an impact in other elements that was not considered. Therefore, besides being cautious about who is given the authority to modify the system model and the timing for the updates, managers should always follow a proper procedure for the management of change, that includes impact analysis. Once the change has been evaluated and approved, the model should be updated. Also, if the change only took place in some instances of the model element and not in all of them, special attention must be paid at the moment of the update to adjust the model accordingly, to avoid the modification of all the instances at once[35].

[35]For example, instead of renaming or modifying the properties of a block that is used in two or more diagrams, which would propagate the changes throughout all the diagrams where it is used, replace it only in the affected diagram with a new block with a different name and/or properties.

4.6 Benefits for managers and regulators

This model is beneficial to managers for many reasons. It can lower the cost of maintaining the documentation of the system. It gives them tools for impact analysis in management of change activities, and consequently, to support decisions related to change. The model can be used in training, and as a way to increase awareness and understanding of the way in which the physical components of the protective system work, the information flows in the management system, the operating procedures and policies established, the requirements from laws, regulation, and recommendations from professional associations and other exerts, the activities to perform with their respective inputs and outputs during each lifecycle stage, and the notion of who the stakeholders are and what are their main roles and concerns.

This model acknowledges governments and regulators as stakeholders of protective systems. Nevertheless, it may also constitute a tool that will help them to mitigate moral hazard, and perform their activities related to the preservation of public safety.

Regulators have the authority to enforce the adoption and use of protective systems. They may also suggest, promote, or demand the use of MBSE to facilitate companies to comply with prescriptive regulation, including OSHA PSM, EPA RMP, as other laws and regulations set as requirements. Adopting MBSE practices may also facilitate audits and inspections, as companies would be able to provide the authorities with the current status of the company in terms of the implementation of protective measures, their processes and equipment.

Furthermore, regulators acquire information and make it available to people who are making social choice decisions. If regularly updated, this model may help them to keep in hand the specific needs and concerns of the near neighbors and general population they seek to protect, which can be summarized and captured as the views and viewpoints of the external affected stakeholders. They need to know what kind of information they

must obtain from safety-critical companies to answer the questions from the public and mitigate moral hazard. Having a model that illustrates the structure and behavior of the protective systems companies use could help them determine what information they should request. Also, companies can be aware of the concerns of the external stakeholders, and create packages with the information to disclose to them, including views of the model understandable and relevant to those audiences, and satisfy the requests of regulators.

5. CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

We have created a MBSE framework that advances the state of the art in safety-critical protective systems, by integrating the management and governance dimensions, and offering further capabilities inherent to the MBSE approach. While it is still consistent with the current characterization of protective systems as a group of protection layers used in LOPA, our model is also suitable for combined design, operation, and regulation; it reduces the cost of maintenance of its artifacts; and offers tools for simulation, impact analysis, and management of change. Potential users include both enterprises and regulators from the chemical process safety industry and the energy sector, and any other agents invested in the design and management of protective systems.

This work significantly reduces the pitfalls of its document-based predecessors, by offering an organic, visual model with traceable, integrated and consistent elements, whose changes automatically propagate throughout every part where the modified element appears, instead of a set of disjoint texts, which are prone to errors, expensive to maintain, or may become inconsistent and obsolete as the system evolves.

This framework includes system governance. It captures the management system that supports the protection layers, as well as the internal policies and applicable regulations, modeled through various blocks, requirements, activities, and information flows between entities. Furthermore, this framework encompasses the views and viewpoints of multiple owners, whose roles vary throughout the system lifecycle, and includes both internal and external stakeholders. Therefore, it supports shared governance, and can be used by multiple agents within and beyond the enterprise premises.

For the same reason, it mitigates information asymmetry, as all of its users share the same model. Nevertheless, it also renders the possibility to provide its specific audiences with tailored views, relevant to them, at different levels of granularity, and filtered according to their respective roles and concerns.

Besides modeling the physical components, management system, policy, laws and regulation, lifecycle, and stakeholders, our framework subsumes two very important aspects in a protective system: impact analyses, and management of change. With regard to impact analyses, it allows the users to identify where each model element is used throughout the diagrams, what elements may affect it, and what other elements it may affect. It also shows other types of existing relations among elements, such as generalizations, to inherit properties from the supertypes to the subtypes; composite and reference associations, to convey aggregations and physical connections; and allocations, to assign behaviors to structures, or establish cross relationships. Knowing these relations helps the users to assess possible impacts in other parts of the model, before making any changes to its elements.

With regard to MOC, our framework models it as part of the management system, hence, it includes the information exchanged with its other elements. MOC is also treated in a special section of the model, which illustrates various MOC guidelines, from key principles and essential features of MOC and the activities to perform during the design and development of a MOC system, to the roles in a MOC team and their interactions as changes are proposed, evaluated, and eventually authorized or denied. As part of the assessment of possible impacts, we suggest a methodical use of the tools for impact analyses provided in our model, that is, a realistic approach to manage multiple aspects of change.

This framework focuses mainly on protective systems' architecture and governance. However, as additional features, it also supports simulation and other analyses, which may be of stochastic or deterministic nature. Potentially, every element in the system structure modeled as a block may possess value properties, and mathematical equations imposed

to them. Users can create instances to input values and solve the equations, or generate thousands of scenarios to evaluate, linked to the model. Therefore, this framework subordinates analytical modeling.

With these computational and analytical capabilities embedded in the model, the users can develop and deploy parametric diagrams, as well as functions and scripts[1] to compute various indicators and perform analyses required by law, and integrate them in the system model. Thus, besides constituting a tool for management and governance, impact analysis and management of change, this framework may allow its users to comply with and support the development of both prescriptive and performance-based regulation.

Standards are essential in engineering. The model of protective systems developed in this research conforms to OMG's and INCOSEs standards[2]. Furthermore, we believe that our model may constitute a beginning point in the development of more sophisticated standards for protective systems. It provides a medium that supports an implementation of the management and governance, in addition to the physical components that constitute the protection layers.

Ex-post civil liability is intended to compensate the victims after catastrophes occur, while *ex-ante* safety regulation aims to induce protective measures to prevent catastrophes. Yet, it is not unusual to find that standards and laws in safety-critical industries are often created as a response to major incidents. Indeed, the development of both prescriptive and performance-based regulation is difficult, and shifting towards the latter is also controversial. Additionally, the role of regulators is not simply limited to issuing safety regulation and verifying its compliance. Regulators synthesize and disseminate information, and serve as an interface and mediator between companies and the general public. This model

[1] In MATLAB M-files or Mathematica c-Mathematica.

[2] OMG and INCOSE are two organizations that issue standards. They extended UML -an international standard specified by the OMG and accepted as an ISO standard (ISO/IEC 19501)- and created SysML as a standard modeling language for systems engineering applications.

can be shared by both industry and regulators, and provides all of its stakeholders with information regarding the structure, behavior, and parameters of protective systems, and offers tools to assess possible impacts of planned and unplanned changes.

Based on the multiple benefits that the use of MBSE provides, at a very low expense, to safety-critical companies and its many stakeholders, including regulators, and ultimately the general population, we conclude it should be a regulatory requirement.

5.2 Future work

There are at least three paths for future work: Improving, extending, adapting and/or refining this model using the same tools as so far, incorporating the use of other software tools to enhance the model capabilities, and using the MBSE approach in non safety-critical areas of application that can benefit from systems engineering.

5.2.1 Improving, extending, adapting or refining this model using the same tools

Our model can be improved in several ways. Virtually any block in the model can be enhanced with further properties in displayed or hidden compartments, to include values, constraints, operations, and receptions, if applicable.

Every use case and activity depicted in the diagrams can be explained in more detail creating other behavioral diagrams that include subroutines or activities to be invoked; or sequence diagrams that show who performs what activity in which order, and how the entities that participate communicate with each other in a certain order; or state machine diagrams that indicate the possible states of the elements of the model, such as the layers of protection and their respective physical components, the status of a request for change, or applicable activities within the management system, as well as what kind of events trigger changes of state.

The emergency response layer, with its corresponding stakeholders, can be extended

to include practices from the incident command system (ICS), which is "a particular approach to assembly and control of the highly reliable temporary organizations employed by many public safety professionals to manage diverse resources at emergency scenes" [4].

Several requirements can be added. Possible sources include federal and state laws, other safety regulations, and best practices from professional associations. Besides its text-based part indicating what shall or should be done, the relationships used in SysML to establish traceability among requirements or traceability from requirements to the structures and behaviors in the system can be included.

Our model has the views and viewpoints of some representative stakeholders, but it does not include views and viewpoints for all of them. Also, many more views and viewpoints that encompass what various groups of stakeholders who belong to different supertypes have in common could be created. Other packages with subsets of the model partitioned following criteria distinct to the lifecycle stages or the condition of input or output can also be created, assuming that doing this would have a valid purpose.

Adapting the model to a specific industry is also a viable alternative. It currently is oriented towards process safety, but although some principles are the same, some physical components, management system parts, policies, and laws and regulation may vary across industries, or be country specific, and have different needs.

The model can be extended to encompass other CCPS guidelines[3], or refined to focus on fewer elements but in greater detail. Given our discussion about management failure as the cause of protective systems failure, and the challenges brought by shared governance and moral hazard, refining the model to focusing more on the management system and the stakeholders is a reasonable alternative.

The example we used for showing the simulation capabilities to perform LOPA can be

[3]Our work was based mostly on 3 out of a over 100 publications.

extended for the general case of n protection layers of any type. It may also be adapted to include the effect of enabling conditions and conditional modifiers.

5.2.2 Incorporating the use of other software tools to enhance the model capabilities

Another path for future work consists of incorporating the use of other software tools to enhance the model capabilities. The creator of the software we used in the construction of our model has recently launched a newer version of a toolkit[4] as an effort to integrate safety and reliability analysis and allow the use of FMEA. LOPA is only one of the many analyses in the qualitative-quantitative spectrum for safety and reliability. There is potential for adding other analyses. This will allow to directly synthesize information for probabilistic risk assessment (PRA) and quantitative risk assessment (QRA).

5.2.3 Using the MBSE approach in other areas

Finally, another possibility for future work consists of using the MBSE approach in other areas of application that are not safety-critical, but can benefit from systems engineering approach.

[4]MBSE toolkit.

REFERENCES

[1] C Abhiram. Case Study Presentation on Piper Alpha and San Juanico Incident. Conference on Chemical (Industrial) Disaster Management (CIDM). http://cidm.in/presentations/C.%20Abhiram,%20IOCL%20%20Case%20Study%20Presentation%20on%20Piper%20Alpha%20and%20San%20Juanico%20Incident.pdf, 2014. Accessed: 2015-02-02.

[2] Laurence Bellagamba. *Systems engineering and architecting : creating formal requirements.* Boca Raton, FL : CRC Press, 2012.

[3] Pierre Bentata. On the joint use of safety regulation and civil liability to promote safe management of hazardous operations: A French case study. *Journal of Risk Research*, 17(6):721–734, 2014.

[4] Gregory A. Bigley and Karlene H. Roberts. The incident command system: High-reliability organizing for complex and volatile task environments. *Academy of Management Journal*, 44(6):1281 – 1299, 2001.

[5] Benjamin S. Blanchard. *System engineering management.* Wiley series in systems engineering and management. Hoboken, NJ : John Wiley & Sons, Incorporated, 2008.

[6] Marcel Boyer and Donatella Porrini. The impact of court errors on liability sharing and safety regulation for environmental/industrial accidents. *International Review of Law & Economics*, 31(1):21 – 29, 2011.

[7] Peter Cane. Tort law as regulation. *Common Law World Review*, 31(4):305 – 331, 2002.

[8] Andrea L. Cassano-Piche, Kim J. Vicente, and Greg A. Jamieson. A test of Rasmussen's risk management framework in the food safety domain: BSE in the UK. *Theoretical Issues in Ergonomics Science*, 10(4):283 – 304, 2009.

[9] Center for Chemical Process Safety. *Guidelines for implementing process safety management systems*. Center for Chemical Process Safety/AIChE, 1994.

[10] Center for Chemical Process Safety. *Plant guidelines for technical management of chemical process safety. Revised edition*. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers, 1995.

[11] Center for Chemical Process Safety. *Guidelines for integrating process safety management, environment, safety, health, and quality*. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers, 1996.

[12] Center for Chemical Process Safety. *Layer of Protection Analysis - Simplified Process Risk Assessment*. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2001.

[13] Center for Chemical Process Safety. *Guidelines for safe and reliable instrumented protective systems*. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2007.

[14] Center for Chemical Process Safety. *Guidelines for the management of change for process safety*. Hoboken, NJ : Wiley-Interscience, 2008.

[15] Center for Chemical Process Safety. *Guidelines for auditing process safety management systems. 2nd ed.* New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2011.

[16] Center for Chemical Process Safety. *Guidelines for enabling conditions and conditional modifiers in layer of protection analysis (LOPA)*. Hoboken, NJ : John Wiley

& Sons, Incorporated, 2014.

[17] Chung-Suk Cho, Young-Ji Byon, Francis Boafo, and Hyunjoo. Kim. Impact analysis of the new OSHA cranes and derricks regulations on crane operation safety. *KSCE Journal of Civil Engineering*, 21(1):1–13, 2016.

[18] Mark A. Cohen. Monitoring and enforcement of environmental policy. http://infohouse.p2ric.org/ref/33/32797.pdf, 1998. Accessed: 2015-02-03.

[19] Daniel A. Crowl and Joseph F. Louvar. *Chemical process safety: fundamentals with applications.* Upper Saddle River, NJ : Prentice Hall, 2011.

[20] Susmita Dasgupta, Benoît Laplante, Nlandu Mamingi, and Hua Wang. Analysis: Inspections, pollution prices, and environmental performance: evidence from China. *Ecological Economics*, 36(3):487 – 498, 2001.

[21] Harvey T. Dearden. Contractual provisions for the supply of safety instrumented systems. *Measurement and Control (United Kingdom)*, 48(1):26–27, 2015.

[22] Lenny Delligatti. *SysML distilled. A brief guide to the systems modeling language.* Upper Saddle River, NJ : Addison-Wesley, 2014.

[23] Donald N. Dewees. The comparative efficacy of tort law and regulation for environmental protection. *The Geneva Papers on Risk and Insurance. Issues and Practice*, 17(65):446 – 467, 1992.

[24] Arthur M. Dowell. Is it really an independent protection layer? *Process Safety Progress*, 30(2):126–131, 2011.

[25] Howard Eisner. *Essentials of project and systems engineering management. 3rd ed.* Hoboken, NJ : John Wiley & Sons, Incorporated, 2008.

[26] Rik Eshuis and Roel Wieringa. *Comparing Petri net and activity diagram variants for workflow modelling–a quest for reactive Petri nets*. Berlin Heidelberg : Springer, 2003.

[27] Michael Faure. Private liability and critical infrastructure. *European Journal of Risk Regulation*, 6(2):229 – 243, 2015.

[28] Federal Aviation Administration. National Airspace System System Engineering Manual. https://www.scribd.com/document/98230420/NAS-Systems-Engineering-Manual-Vol-1, 2016. Accessed: 2016-08-30.

[29] Jérôme Foulon, Paul Lanoie, and Benoît Laplante. Regular article: Incentives for pollution control: Regulation or information?. *Journal of Environmental Economics and Management*, 44(1):169 – 187, 2002.

[30] Sanford Friedenthal, Alan Moore, and Rick Steiner. *A practical guide to SysML : the systems modeling language.* Waltham, MA : Morgan Kaufman, 2015.

[31] Wayne B. Gray and Mary E. Deily. Compliance and enforcement: Air pollution regulation in the U.S. steel industry. *Journal of Environmental Economics and Management*, 31(1):96 – 111, 1996.

[32] Dave Hall, Rob Jones, Carlo Raffo, and Alain Anderton. *Business Studies*. London : Pearson, 2008.

[33] James T. Hamilton. Pollution as news: Media and stock market reactions to the toxics release inventory data. *Journal of Environmental Economics and Management*, 28(1):98 – 113, 1995.

[34] Arifumi Hasegawa, Koichi Tanigawa, Akira Ohtsuru, Hirooki Yabe, Masaharu Maeda, Jun Shigemura, Tetsuya Ohira, Takako Tominaga, Makoto Akashi, Nobuyuki Hirohashi, Tetsuo Ishikawa, Kenji Kamiya, Kenji Shibuya, Shunichi Yamashita, and

Rethy K Chhem. Series: Health effects of radiation and other health problems in the aftermath of nuclear accidents, with an emphasis on Fukushima. *The Lancet*, 386(9992):479 – 488, 2015.

[35] Herbert W. Heinrich. *Industrial accident prevention : a scientific approach. 2nd ed.* New York, NY : McGraw-Hill, 1941.

[36] Jon Holt. *UML for systems engineering : watching the wheels. 2nd ed.* London : Institution of Electrical Engineers, 2004.

[37] Jon Holt and Simon Perry. *SysML for systems engineering - A model-based approach. 2nd ed.* London : The Institution of Engineering and Technology, 2014.

[38] Keith N. Hylton. When should we prefer tort law to environmental regulation?. *Washburn Law Journal*, 41(3):515 – 534, 2002.

[39] International Atomic Energy Agency. Communication with the public. https://www.iaea.org/ns/tutorials/regcontrol/commun/com811.htm, 2002. Accessed: 2016-6-6.

[40] International Atomic Energy Agency. Legislative and regulatory framework. https://www.iaea.org/ns/tutorials/regcontrol/legis/legis135.htm, 2016. Accessed: 2016-10-9.

[41] Hamid Jahanian and Adam Lucas. The role of component arrangement in complex safety instrumented systems - a case study. *Process Safety and Environmental Protection*, 94(C):113–130, 2015.

[42] David C. Jensen and Irem Y. Tumer. Modeling and analysis of safety in early design. *Procedia Computer Science*, 16(2013 Conference on Systems Engineering Research):824 – 833, 2013.

[43] Abraham Almaw Jigar, Yiliu Liu, and Mary Ann Lundteigen. Spurious activation analysis of safety-instrumented systems. *Reliability Engineering & System Safety*, 156:15 – 23, 2016.

[44] Matthew E. Kahn. Environmental disasters as risk regulation catalysts? The role of Bhopal, Chernobyl, Exxon Valdez, Love Canal, and Three Mile Island in shaping U.S. environmental law. *Journal of Risk and Uncertainty*, 35(1):17 – 43, 2007.

[45] Alvin Kaufman and Karen K. Nelson. *Three Mile Island : Who pays the bill?*. Major studies and issue briefs of the Congressional Research Service: Supplement 1982-83, reel 4, fr. 0147. Washington, DC : Library of Congress, Congressional Research Service, 1982.

[46] Shameek Konar and Mark A. Cohen. Information as regulation: The effect of community right to know laws on toxic emissions. *Journal of Environmental Economics and Management*, 32(1):109 – 124, 1997.

[47] Paul R. Krugman. *The return of depression economics and the crisis of 2008. 1st ed.* New York, NY : W.W. Norton & Company, 2009.

[48] William M. Landes and Richard A. Posner. *The economic structure of tort law.* Cambridge, MA : Harvard University Press, 1987.

[49] Paul Lanoie, Benoît Laplante, and Maité Roy. Can capital markets create incentives for pollution control?. *Ecological Economics*, 26(1):31, 1998.

[50] Benoît Laplante and Paul Rilstone. Environmental inspections and emissions of the pulp and paper industry in Quebec. *Journal of environmental economics and management*, 31(1), 1996.

[51] Nancy Leveson. The Drawbacks in Using The Term 'System of Systems' biomedical instrumentation and technology. http://sunnyday.mit.edu/papers/system-of-

systems.pdf, 2013. Accessed: 2015-09-30.

[52] Yiliu Liu and Marvin Rausand. Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems. *Reliability Engineering & System Safety*, 145:366 – 372, 2016.

[53] Antonio Eduardo Bier Longhi, Artur Alves Pessoa, and Pauli Adriano de Almada Garcia. Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees. *Reliability Engineering & System Safety*, 142:525–538, 2015.

[54] Wesley A. Magat and W. Kip Viscusi. Effectiveness of the EPA's regulatory enforcement: The case of industrial effluent standards. *The Journal of Law & Economics*, 33(2):331–360, 1990.

[55] Arun S. Malik. Optimal environmental regulation based on more than just emissions. *Journal of Regulatory Economics*, 32(1):1 – 16, 2007.

[56] Marsh-Ltd. The 100 Largest Losses 1974-2013. Large Property Damage Losses in the Hydrocarbon Industry. 23rd Edition. https://uk.marsh.com/Portals/18/Documents/100%20Largest%20Losses%2023rd%20Edition%202014.pdf, 2014. Accessed: 2015-02-02.

[57] Marsh-Ltd. The 100 Largest Losses 1974-2015. Large Property Damage Losses in the Hydrocarbon Industry. 24rd Edition. https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/100%20largest%20losses%201974%20to%202015-03-2016.pdf, 2016. Accessed: 2016-06-10.

[58] Chad McGuire, Jessica Lo, and Erik Mathiason. Selecting sensors for safety instrumented systems. *Chemical Engineering Progress*, 111(7):20 – 25, 2015.

[59] Peter S. Menell. A note on private versus social incentives to sue in a costly legal system. *The Journal of Legal Studies*, 12(1):41 – 52, 1983.

[60] Abdelhak Mkhida, Jean-Marc Thiriet, and Jean-Franois Aubry. Integration of intelligent sensors in safety instrumented systems (SIS). *Process Safety and Environmental Protection*, 92(2):142 – 149, 2014.

[61] Louis W. Nadeau. EPA effectiveness at reducing the duration of plant-level noncompliance. *Journal of Environmental Economics and Management*, 34(1):54 – 78, 1997.

[62] NASA. *Systems engineering handbook.* Washington, DC : National Aeronautics and Space Administration, 2007.

[63] Object Management Group Inc. OMG Systems Modeling Language (OMG SysML) Version 1.4. http://www.omg.org/spec/SysML/1.4/PDF/, 2015. Accessed: 2016-05-13.

[64] Office of the Deputy Assistant Secretary of Defense. Systems Engineering. http://www.acq.osd.mil/se/initiatives/init_pp-sse.html, 2016. Accessed: 2016-08-30.

[65] Anthony I. Ogus. *Regulation : legal form and economic theory.* Oxford : Clarendon Press ; New York : Oxford University Press, 1994.

[66] Maryam Rahimi and Marvin Rausand. Monitoring human and organizational factors influencing common-cause failures of safety-instrumented system during the operational phase. *Reliability Engineering & System Safety*, 120:10 – 17, 2013.

[67] Jens Rasmussen. Risk management in a dynamic society: A modelling problem. *Safety Science*, 27(2-3):183 – 213, 1997.

[68] Dave Rebbitt. Pyramid power. *Professional Safety*, 59(9):30 – 34, 2014.

[69] Karlene H. Roberts. Managing high reliability organizations. *California Management Review*, 32(4):101 – 113, 1990.

[70] Karlene H. Roberts. Some characteristics of one type of high reliability organization. *Organization Science*, 1(2):160 – 176, 1990.

[71] Karlene H. Roberts and Robert G. Bea. When systems fail. *Organizational Dynamics*, 29(3):179, 2001.

[72] Karlene H. Roberts and Carolyn Libuser. From Bhopal to banking: Organizational design can mitigate risk. *Organizational Dynamics*, 21(4):15 – 26, 1993.

[73] Susan Rose-Ackerman. Regulation and the law of torts. *The American Economic Review*, 81(2):54 – 58, 1991.

[74] Roy E. Sanders. *Chemical process safety : learning from case histories. 3rd ed.* Amsterdam ; Boston, MA : Elsevier Butterworth Heinemann, 2005.

[75] Patrick W. Schmitz. On the joint use of liability and safety regulation. *International Review of Law & Economics*, 20(3):371 – 382, 2000.

[76] Jon T. Selvik and E.B. Abrahamsen. How to classify failures when collecting data for safety-instrumented systems in the oil and gas industry. *Journal of Risk Research*, 0(0):1–11, 2016.

[77] Steven Shavell. Strict liability versus negligence. *The Journal of Legal Studies*, 9(1):1 – 25, 1980.

[78] Steven Shavell. Liability for harm versus regulation of safety. *The Journal of Legal Studies*, 13(2):357 – 374, 1984.

[79] Angela E. Summers and William H. Hearn. Risk criteria, protection layers, and conditional modifiers. *Process Safety Progress*, 31(2):139–144, 2012.

[80] Alejandro C. Torres-Echeverría, Sebastián Martorell, and Haydn A. Thompson. Modelling and optimization of proof testing policies for safety instrumented systems. *Reliability Engineering & System Safety*, 94(4):838 – 854, 2009.

[81] Margaret J. Trotter, Paul M. Salmon, and Michael G. Lenn. Impromaps: Applying Rasmussen's risk management framework to improvisation incidents. *Safety Science*, 64:60 – 70, 2014.

[82] U.S. Department of Labor. Occupational Safety and Health Administration. Process Safety Management. https://www.osha.gov/Publications/osha3132.html, 2000. Accessed: 2016-03-15.

[83] U.S. GPO. Part 401 Organization and definitions. http://www.gpo.gov/fdsys/pkg/CFR-2011-title14-vol4/pdf/CFR-2011-title14-vol4-sec401-5.pdf, 2011. Accessed: 2015-08-15.

[84] U.S. Nuclear Regulatory Commission. Performance-Based Regulation. http://www.nrc.gov/reading-rm/basic-ref/glossary/performance-based-regulation.html, 2016. Accessed: 2016-10-9.

[85] U.S. Senate, Committee on Environment and Public Works, Subcommittee on Clean Air and Nuclear Safety. *Three Mile Island : looking back on 30 years of lessons learned : hearing before the Subcommittee on Clean Air and Nuclear Safety of the Committee on Environment and Public Works, United States Senate, One Hundred Eleventh Congress, first session, March 24, 2009.* Washington : U.S. Government Publishing Office, 2015.

[86] Annette L. Vietti-Cook. White Paper on Risk-Informed and Performance-Based Regulation. http://www.nrc.gov/reading-rm/doc-collections/commission/srm/1998/1998-144srm.pdf, 1999. Accessed: 2016-10-9.

[87] David D. Walden, Garry J. Roedler, Kevin Forsberg, R. Douglas Hamelin, and Thomas M. Shortell. *Systems engineering handbook : a guide for system life cycle processes and activities. 4th ed.* Hoboken, NJ : John Wiley & Sons, Incorporated, 2015.

[88] Agnieszka Wegrzyn, Andrei Karatkevich, and Jacek Bieganowski. Detection of deadlocks and traps in Petri nets by means of Thelen's prime implicant method. *International Journal of Applied Mathematics and Computer Science*, 14(1):113 – 121, 2004.

[89] Tim Weilkiens. *Systems engineering with SysML / UML : modeling, analysis, design.* Amsterdam ; Boston, MA : Morgan Kaufmann OMG Press / Elsevier, 2007.

[90] Kristina S. Westerdahl. Societal consequences of radioactive releases in March 2011 in Japan and implications for the resilience concept. *Journal of Risk Research*, 17(9):1147 – 1160, 2014.

APPENDIX A

DIAGRAMS

Diagrams 1 through 55, discussed in section 4, are included as a separate file. See *Diagrams.pdf*.

Diagram 1. Protection layers.

Diagram 2. Initiating causes.

Diagram 3. Protection layers exploded.

Diagram 4. Relief system with behaviors allocated to structures.

Diagram 5. Physical components.

Diagram 6. Management system.

Diagram 7. Asset integrity.

Diagram 8. Audits.

Diagram 9. Contractor management.

Diagram 10. Documents and documentation policies.

Diagram 11. Emergency planning and response.

Diagram 12. Hazard analysis.

Diagram 13. Human factors.

Diagram 14. Incident investigation.

Diagram 15. Management of change.

Diagram 16. Operating procedures.

Diagram 17. Pre-startup review.

Diagram 18. Process safety information compilation.

Diagram 19. Risk assessment.

Diagram 20. Training.

APPENDIX B

MAIN MODEL ELEMENTS

A list of the main elements of the model presented in section 4 is included as a separate file. See *Main Model Elements.pdf*.